Raritan EMX

Benutzerhandbuch
Version 2.1.0

Copyright © 2012 Raritan, Inc.

EMX-0C-v2.1-G

März 2012

255-80-6107-00

Dieses Dokument enthält proprietäre Informationen, die durch Urheberrechtsgesetze geschützt sind. Alle Rechte vorbehalten. Dieses Dokument darf ohne die vorherige schriftliche Zustimmung der Raritan, Inc., weder ganz noch teilweise fotokopiert, reproduziert oder in eine andere Sprache übersetzt werden.

© Copyright 2012 Raritan, Inc. Die in diesem Dokument genannte Software und Hardware anderer Hersteller sind registrierte Marken oder Marken sowie Eigentum der jeweiligen Inhaber.

FCC-Informationen

Dieses Produkt wurde getestet und erfüllt die Grenzwerte für ein digitales Gerät der Klasse A entsprechend Abschnitt 15 der FCC-Bestimmungen. Diese Grenzwerte sollen einen angemessenen Schutz vor schädlichen Störungen in einem kommerziellen Umfeld bieten. Dieses Gerät erzeugt, verwendet und sendet Hochfrequenzsignale und kann bei unsachgemäßer Installation und Nichtbefolgung der Anweisungen zu Störungen des Funkverkehrs führen. Der Betrieb dieses Produkts in einem Wohngebiet kann zu Störungen führen.

VCCI-Informationen (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan ist nicht haftbar für Schäden an diesem Produkt, die durch Versehen, Unglück, unsachgemäßen Gebrauch, Missbrauch, nicht von Raritan vorgenommene Änderungen am Produkt oder andere Ereignisse entstehen, die nicht mit zumutbarem Aufwand von Raritan kontrolliert werden können oder unter normalen Betriebsbedingungen nicht eintreten.

Inhalt

Kapitel 1 Einführung 1

Übersicht 2
Produktmodelle 3
EMX2-111 3
EMX2-888 3
Produktfeatures 4
Paketinhalt 5

Kapitel 2 Installieren und Konfigurieren des EMX-Geräts 6

Vorbereitende Schritte 6
Montieren des EMX-Geräts 6
Montage eines Null-U-EMX-Geräts 7
Montage eines 1U-EMX-Geräts 8
Anschließen der EMX-Einheit an eine Stromquelle 10
Konfigurieren der EMX-Einheit 11
Anschließen der EMX-Einheit an einen Computer 11
Installieren des USB-Seriell-Treibers 12
Anschließen der EMX-Einheit an das Netzwerk 13
Erstkonfiguration des Netzwerks 14
Verknüpfen von Assetsensoren 22
Anschließen von Assetsensoren an das EMX-Gerät 24
Anschließen von AMS-M2-Z-Assetsensoren (optional) 26
Anschließen von Blade-Erweiterungsstrips 28
Anschließen der Umgebungssensoren (optional) 31
Informationen zu Kontaktschlusssensoren 33
Anschluss von Detektoren/Switches anderer Hersteller 33
LEDs des Kontaktschlusssensors 37
Anschließen von Differenzluftdrucksensoren 38
Anschluss einer Logitech-Webcam (optional) 39
Anschluss eines Schroff LHX-Wärmetauschers (optional) 40

Kapitel 3 Einführung 41

Unterstützte Webbrowser 41
Anschluss-Ports 41
LCD-Anzeigefeld 43
LCD-Anzeige 43
Bedienelemente 45

Reset-Taste 49
Anschluss des Kontaktschlusssensors 49
Netzschalter 49
Anmelden 50
Abmelden 51
Ändern des Kennworts 52
Einführung in die Webschnittstelle 53
Menüs 54
Schaltfläche "Setup" (Einrichten) 54
Statusleiste 54
Symbol "Add Page" (Seite hinzufügen) 56
Datenfenster 57
Warnsymbol 57
Gelb oder Rot hervorgehobene Ergebnisse 58
Durch den Browser definiertes Kontextmenü 60
Anzeigen des Dashboards 61

Kapitel 4 Verwaltung von Benutzern und Benutzerfunktionen 62

Übersicht 62
Verwalten von Benutzern 62
Erstellen von Benutzerprofilen 62
Ändern von Benutzerprofilen 67
Löschen von Benutzerprofilen 68
Ändern der Ansicht der Benutzerliste 68
Anzeigen der verbundenen Benutzer 68
Verwalten von Benutzerfunktionen 70
Einrichten von Benutzerfunktionen 70
Erstellen einer Benutzerfunktion 70
Ändern von Benutzerfunktionen 71
Löschen einer Benutzerfunktion 73

Kapitel 5 EMX-Geräteverwaltung 74

Übersicht 74
Benennen des EMX-Geräts 74
Anzeigen der Geräteinformationen 75
Einstellen von Datum und Uhrzeit 75
Festlegen der Höhe des Geräts über Normal-Null 77
Ändern der Maßeinheiten 78
Festlegen der Anzeige von Elementen in der Verzeichnisstruktur 79
Anzeigen von Assetsensoren 79
Anzeigen von LHX-Wärmetauschern 80
Ändern der Netzwerkkonfiguration 81
Ändern der Netzwerkschnittstelleneinstellungen 81
Ändern der Netzwerkeinstellungen 84
Ändern der Netzwerkdiensteinstellungen 89
Ändern der HTTP(S)-Einstellungen 89
Konfigurieren der SNMP-Einstellungen 90
Ändern der SSH-Einstellungen 90

Ändern der Telnet-Einstellungen 91
Aktivieren der Dienstbekanntmachung 92
Konfigurieren der SMTP-Einstellungen 93
Einrichten einer EMX-Einheit mit der Sammelkonfiguration 94
Speichern einer EMX-Konfiguration 95
Kopieren einer EMX-Konfiguration 96
Firmware-Upgrade 96
Aktualisieren der Firmware 97
Anzeigen des Protokolls zur Firmwareaktualisierung 98
Vollständige Notfallwiederherstellung 99
Aktualisieren der Assetsensor-Firmware 99
Netzwerkdiagnose 99
Überprüfen eines Hosts mit dem Ping-Tool 100
Verfolgen der Netzwerkroute 100
Auflisten von TCP-Verbindungen 101
Herunterladen von Diagnoseinformationen 101
Neustart des EMX-Geräts 102
Wiederherstellen der werksseitigen Standardeinstellungen 103

Kapitel 6 Security (Sicherheit) 104

Zugriffssteuerung 104
Erzwingen der HTTPS-Verschlüsselung 104
Konfigurieren der Firewall 105
Einrichten von Benutzeranmeldesteuerungen 112
Einrichten von benutzerfunktionsbasierten Zugriffssteuerungsregeln 116
Einrichten eines SSL-Zertifikats 122
Certificate Signing Request (CSR) 122
Erstellen eines selbstsignierten Zertifikats 125
Installieren vorhandener Schlüssel- und Zertifikatsdateien 127
Herunterladen von Schlüssel- und Zertifikatsdateien 128
Einrichten der LDAP-Authentifizierung 129
Ermitteln der LDAP-Informationen 129
Hinzufügen der LDAP-Servereinstellungen 130
Sortieren der Reihenfolge für den LDAP-Zugriff 133
Testen der LDAP-Serververbindung 134
Bearbeiten der LDAP-Servereinstellungen 134
Löschen der LDAP-Servereinstellungen 135
Deaktivieren der LDAP-Authentifizierung 135
Aktivieren der LDAP- und lokalen Authentifizierungsdienste 136

Kapitel 7 Ereignisregeln, Ereignisaktionen und Anwendungsprotokolle 137

Ereignisregeln und Aktionen 137
Komponenten einer Ereignisregel 138
Erstellen einer Ereignisregel 138
Beispiel-Ereignisregeln 161
Ändern einer Ereignisregel 164
Ändern einer Aktion 165
Löschen einer Ereignisregel oder Aktion 166

Hinweis zu nicht ausgelösten Regeln 166
Ereignisprotokollierung 166
Anzeigen des lokalen Ereignisprotokolls 167
Löschen von Ereigniseinträgen 168
Anzeigen des Kommunikationsprotokolls 168

Kapitel 8 Verwalten externer Geräte 170

Übersicht 170
Serverzugriff 170
Hinzufügen von IT-Geräten zur Ping-Überwachung 170
Bearbeitung der Einstellungen zur Ping-Überwachung 172
Löschen der Einstellungen zur Ping-Überwachung 172
Überprüfen des Serverüberwachungsstatus 173
Umgebungssensoren 173
Festlegen von Umgebungssensoren 174
Verwalten von Umgebungssensoren 176
Konfigurieren von Umgebungssensoren 177
Einrichten der Datenprotokollierung 181
Anzeigen von Sensordaten 183
Aufheben der Verwaltung von Umgebungssensoren 188
Schwellenwertinformationen 189
Was ist Deassertionshysterese? 189
Was ist das Assertionszeitlimit? 190
Assetsensoren und -Tags 191
Konfigurieren des Assetsensors 191
Ändern der Farbeinstellungen einer bestimmten LED 194
Anschließen von AMS-M2-Z-Assetsensoren (optional) 195
Erweitern eines Blade-Erweiterungsstrips 197
Anschließen von Blade-Erweiterungsstrips 199
Webcams 202
Konfigurieren von Webcams 203
Anzeigen von Webcam-Momentaufnahmen und -Videos 204
Erfassen, Anzeigen und Verwalten von Webcam-Momentaufnahmen 205
Senden von Videos in einer E-Mail oder Sofortnachricht 207
GSM-Modems 208
Schroff LHX-Wärmetauscher 209
Aktivieren und Deaktivieren der Unterstützung für Schroff LHX-Wärmetauscher 210
Benennen eines Wärmetauschers 210
Konfigurieren von Temperatur- und Lüfterschwellenwerten 211
Überwachen des Wärmetauschers 212
Steuern des Wärmetauschers 215

Kapitel 9 Verwenden von SNMP 217

Aktivieren von SNMP 217
Konfigurieren der Benutzer für die verschlüsselte SNMP-V3-Kommunikation 218
Konfigurieren von SNMP-Traps 219
SNMP-GET- und SET-Befehle 220
Die EMX-MIB 220

Kapitel 10 Verwenden der Befehlszeilenschnittstelle 224

Informationen zur Schnittstelle 224
Anmelden bei der CLI 225
Mit HyperTerminal 225
Mit SSH oder Telnet 226
Unterschiedliche CLI-Modi und -Eingabeaufforderungen 227
Schließen einer seriellen Verbindung 227
Befehl "help" 228
Anzeigen von Informationen 228
Netzwerkkonfiguration 228
Einstellungen von Assetsensoren 231
Informationen zum Umgebungssensor 232
Informationen zum Umgebungssensor 233
Schwellenwertinformationen zum Umgebungssensor 234
Security Settings (Sicherheitseinstellungen) 235
Bestehende Benutzerprofile 235
Bestehende Benutzerfunktionen 236
Einstellungen von Rackeinheiten eines Assetsensors 237
Einstellungen für einen Blade-Erweiterungsstrip 238
Befehlsverlauf 238
Größe des Verlaufspuffers 239
Beispiele 239
Konfigurieren von EMX-Gerät und Netzwerk 240
Aufrufen des Konfigurationsmodus 240
Befehle zur Gerätekonfiguration 241
Befehle für die Netzwerkkonfiguration 244
Befehle für die Sicherheitskonfiguration 268
Befehle für die Umgebungssensorkonfiguration 292
Befehle für die Konfiguration von Umgebungssensorschwellenwerten 296
Befehle zur Benutzerkonfiguration 302
Befehle zur Konfiguration von Benutzerfunktionen 317
Befehle zur Assetverwaltung 322
Festlegen der Größe eines Verlaufspuffers 330
Multi-Befehlssyntax 330
Beenden des Konfigurationsmodus 331
Aufheben der Sperrung eines Benutzers 331
Zurücksetzen der EMX-Einheit 332
Neustart des Geräts 332
Wiederherstellen der werksseitigen Standardeinstellungen 333
Behebung von Netzwerkproblemen 333
Aufrufen des Diagnosemodus 333
Diagnosebefehle 333
Beenden des Diagnosemodus 336

Abfragen verfügbarer Parameter für einen Befehl 337
Abrufen vorheriger Befehle 337
Automatisches Vervollständigen eines Befehls 337
Abmelden bei der CLI 338
Wiederherstellen der werksseitigen Standardeinstellungen (CLI) 338

Anhang A Asset-Management bei Dominion PX 339

Übersicht 339

Anhang B Spezifikationen 341

Faktoren zur Höhenkorrektur (EMX) 341
Maximale Umgebungstemperatur für den Betrieb (EMX) 342
Pinbelegung des seriellen RS-232-Ports 342
RJ-12-Pin-Belegung 342
Pinbelegung des RS-485-Ports 343

Anhang C Veranschaulichung der LDAP-Konfiguration 344

Schritt A. Festlegen der Benutzerkonten und Gruppen 344
Schritt B. Konfigurieren der Benutzergruppen auf dem AD-Server 345
Schritt C. Konfigurieren der LDAP-Authentifizierung auf dem EMX-Gerät 346
Schritt D. Konfigurieren der Benutzergruppen auf dem EMX-Gerät 349

Index 353

Kapitel 1 Einführung

In diesem Kapitel

Übersicht....2
Produktmodelle....3
Produktfeatures....4
Paketinhalt....5

Übersicht

Das EMX-Gerät stellt eine Rackverwaltungslösung bereit, die Asset-Management- und Umgebungsüberwachungsfunktionen vereint.

Mit der Asset-Management-Funktion können Sie IT-Gerätestandorte über Fernzugriff verfolgen, nachdem Sie die IT-Geräte elektronisch getaggt haben. Dieses Feature ist besonders hilfreich, wenn Hunderte von IT-Geräte verwaltet werden müssen.

Folgende Komponenten sind zum Einrichten eines Asset-Management-Systems erforderlich:

- Asset-Tags von Raritan: Ein IT-Gerät wird getaggt, indem Sie ein elektronisches Asset-Tag am Gerät befestigen.
- Asset-Management-Sensoren (Assetsensoren) von Raritan: Jeder Assetsensor überträgt Informationen zum Tag und zur Position an das EMX-Gerät.
- Ein EMX-Gerät: Sie können jedes getaggte IT-Gerät über das EMX-Gerät remote aufspüren.

Wenn Raritan-Umgebungssensoren an das EMX-Gerät angeschlossen sind, können Sie die Umgebungsbedingungen (z. B. Temperatur und Feuchtigkeit) im Rechenzentrum oder Serverraum über Fernzugriff überwachen.

Durch den Anschluss einer Logitech® QuickCam® Pro 9000-Webcam entsteht ein einfaches Kamera- und Videoüberwachungssystem, das Echtzeit-Momentaufnahmen oder -Videos aus dem Serverraum oder Rechenzentrum liefert, um die Überwachung zu verbessern und die Sicherheit zu erhöhen.

Bei Eintritt eines Ereignisses ausgelöste Ereignisse und Aktionen werden von der EMX-Einheit unterstützt. Es können insbesondere E-Mail-Nachrichten, Protokollereignisse, Syslog-Meldungen, Webcam-Momentaufnahmen, SNMP-Traps und SMS-Nachrichten ausgelöst werden, wenn die von Ihnen definierten Ereignisse eintreten. Für E-Mail-Nachrichten können benutzerdefinierte Nachrichten konfiguriert und von der Webcam aufgenommene Bilder können per E-Mail an Benutzer gesendet werden.

Zusätzlich kann das EMX-Gerät mit einem Schroff® LHX-20- oder LHX-40-Wärmetauscher kombiniert werden, der warme Luft in den Luft-/Wasser-Wärmetauscher saugt, um die Luft zu kühlen. Diese Integration bietet eine Lösung zur Remote-Überwachung des Wärmetauschers. Die EMX-Einheit kann auch in Verbindung mit der Raritan-Verwaltungsanwendung für Rechenzentren, dcTrack™, verwendet werden.

In diesem Benutzerhandbuch werden folgende Modelle beschrieben:

- EMX2-111

- EMX2-888

Produktmodelle

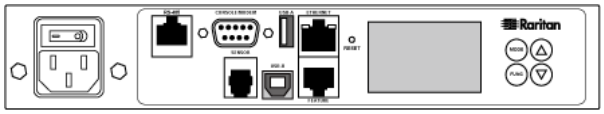
EMX-Geräte gibt es in zwei Modellvarianten: EMX2-111 und EMX2-888.

Die verschiedenen Modelle sind von der Funktion her identisch, unterscheiden sich aber in der Größe und der Gesamtanzahl der Ports.

EMX2-111

EMX2-111 ist ein Null-U-Modell mit den folgenden Ports und Komponenten:

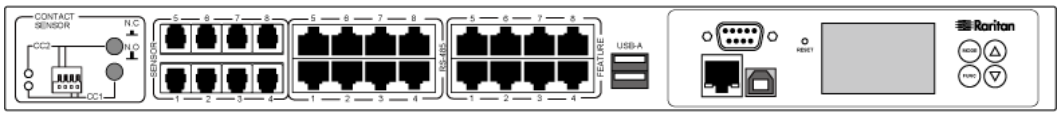
- 1 Sensorport
- 1 Feature-Port
- 1 RS-485-Port
- 2 USB-Ports (1 USB-A und 1 USB-B)
- 1 RS-232-Port
- 1 Ethernet-Port
- 1 LCD-Anzeige
- Bedienelementen



EMX2-888

EMX2-888 ist ein 1-U-Modell mit den folgenden Ports und Komponenten:

- 8 Sensorports
- 8 Feature-Ports
- 8 RS-485-Ports
- 3 USB-Ports (2 USB-A und 1 USB-B)
- 1 RS-232-Port
- 1 Ethernet-Port
- 1 LCD-Anzeige
- Bedienelementen
- Anschluss für Kontaktschlusssensor



Produktfeatures

Generell verfügt das EMX-Gerät über folgende Features:

- Remote-Verfolgung des Standorts der einzelnen IT-Geräte, die mithilfe von Asset-Tags von Raritan elektronisch getaggt ist
- LED-Farbänderung am Assetsensor, um zwischen erkannten und nicht erkannten Asset-Tags zu unterscheiden
- Unterstützung für maximal 10 Meter Verkabelung bei Modell EMX-888 und 1 Meter Verkabelung bei Modell EMX-111 für jeden angeschlossenen Assetsensor
- Überwachen von Umgebungsbedingungen, wie z. B. externe Temperatur und Luftfeuchtigkeit
- Benutzerdefinierbare Standortattribute für Umgebungssensoren
- Möglichkeit, je nach Benutzeranmeldeinformationen Temperaturen in Celsius oder Fahrenheit, Höhen in Meter oder Fuß und Druck in Pascal oder psi anzuzeigen
- Unterstützung für maximal 130 Umgebungssensoren bei Modell EMX-888 und 16 bei Modell EMX-111
- Unterstützung für das Hintereinanderschalten von AMS-Geräten und/oder PX2-Geräten, die an die EMX-Einheit angeschlossen sind
- Unterstützung für SNMP V1, V2 und V3
- Senden von Traps mit dem SNMP-Protokoll
- Konfiguration und Definition von Werten über SNMP
- Unterstützung für SSH- und Telnet-Dienste
- Bei SSH werden sowohl die Kennwortauthentifizierung als auch die Authentifizierung mit öffentlichem Schlüssel unterstützt
- Unterstützung der Dienstbekanntmachung
- Speichern der Konfigurationseinstellungen eines EMX-Geräts und Bereitstellen dieser Einstellungen für andere identische EMX-Geräte
- Unterstützung des Neigungssensors, der in den Assetsensoren von Raritan implementiert ist
- Drahtlose Verbindung über einen von Raritan bereitgestellten drahtlosen USB-LAN-Adapter
- Visuelle Überwachung der Rechenzentrumsumgebung über eine angeschlossene Logitech® QuickCam® Pro 9000-Webcam
- Unterstützung für Webcam-Bilder, die per E-Mail an angegebene Empfänger gesendet werden
- Unterstützung von Cinterion® MC52i GSM-Modems, mit denen Sie angepasste SMS-Nachrichten für bestimmte Ereignisse an angegebene Empfänger senden können

- Senden von E-Mails, Protokollieren von Details und/oder Festlegen von SNMP-Traps für bestimmte Ereignisse
- Überwachung eines angeschlossenen Schroff® LHX-20- oder LHX-40-Wärmetauschers
- Möglichkeit zur Diagnose des Netzwerks, z. B. Anpingen eines Hosts oder Auflisten von TCP-Verbindungen
- Die Möglichkeit, den Serverzugriff zu überwachen
- Option zur vollständigen Notfallwiederherstellung bei Sprungvollausfall während der Firmwareaktualisierung

Paketinhalt

Im Folgenden werden die mit einem EMX-Gerät gelieferten Komponenten beschrieben. Falls ein Teil fehlt oder beschädigt ist, wenden Sie sich an den technischen Kundendienst von Raritan.

- EMX-Gerät
- Netzkabel
- Halterungen und Schrauben
- Assetsensoren (optional)
- Asset-Tags (optional)

Kapitel 2 Installieren und Konfigurieren des EMX-Geräts

In diesem Kapitel

Vorbereitende Schritte 6
Montieren des EMX-Geräts 6
Anschließen der EMX-Einheit an eine Stromquelle 10
Konfigurieren der EMX-Einheit 11
Verknüpfen von Assetsensoren 22
Anschließen von Assetsensoren an das EMX-Gerät 24
Anschließen von AMS-M2-Z-Assetsensoren (optional) 26
Anschließen von Blade-Erweiterungsstrips 28
Anschließen der Umgebungssensoren (optional) 31
Anschließen von Differenzluftdrucksensoren 38
Anschluss einer Logitech-Webcam (optional) 39
Anschluss eines Schroff LHX-Wärmetauschers (optional) 40

Vorbereitende Schritte

Bereiten Sie die Installationsumgebung vor. Stellen Sie sicher, dass die Umgebung, in der die Installation erfolgt, sauber ist und keinen extremen Temperaturen oder hoher Luftfeuchtigkeit unterliegt. Lassen Sie im Umfeld des EMX-Geräts ausreichend Platz für die Kabel und Assetsensor-Verbindungen.

Montieren des EMX-Geräts

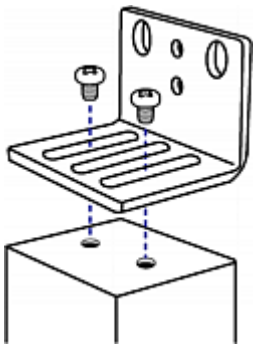
Die Montage des EMX-Geräts variiert abhängig vom erworbenen Modell.

Montage eines Null-U-EMX-Geräts

In diesem Abschnitt wird die Montage eines Null-U-EMX-Geräts mithilfe von L-Halterungen und zwei Knöpfen beschrieben.

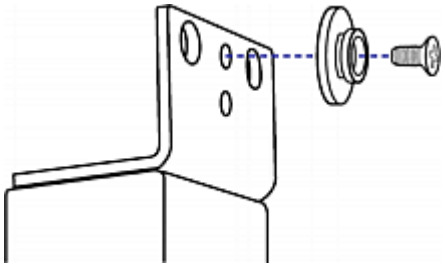
So montieren Sie Null-U-Modelle mithilfe von L-Halterungen und zwei Knöpfen:

1. Richten Sie die beiden äußeren Öffnungen der L-Halterung an den beiden Schraubenöffnungen auf der Oberseite des EMX-Geräts aus.
2. Schrauben Sie die L-Halterung an das Gerät, und stellen Sie sicher, dass die Halterung fest sitzt.



3. Wiederholen Sie die Schritte 1 und 2, um die andere L-Halterung an der Unterseite des Geräts anzuschrauben.
4. Nachdem beide L-Halterungen am Gerät befestigt sind, haben Sie zwei Möglichkeiten, das Gerät im Rack zu montieren.
   - Befestigen Sie das Gerät, indem Sie die Rackschrauben durch die beiden identischen Öffnungen nahe der Kante jeder L-Halterung drehen.

- Befestigen Sie das Gerät, indem Sie einen Rastknopf in der Mitte der Rückseite jeder L-Halterung befestigen und anschließend beide Knöpfe in den Befestigungsöffnungen des Racks einrasten lassen. Das empfohlene Anzugsmoment für den Rastknopf ist 1,96 N·m (20 kgf·cm).



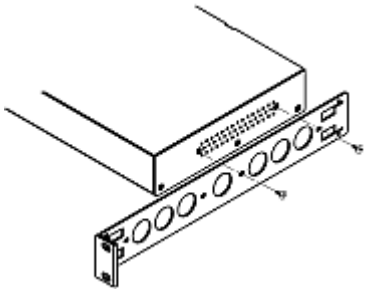
Montage eines 1U-EMX-Geräts

Befestigen Sie das 1U-EMX-Gerät mithilfe der entsprechenden Halterungen und Werkzeuge am Rack oder Schrank.

So montieren Sie das 1U-EMX-Gerät:

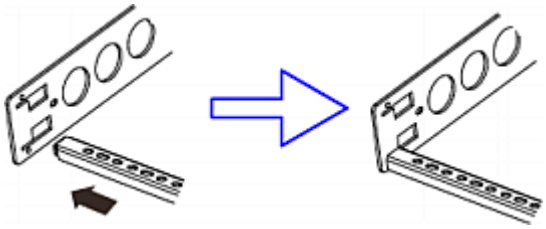
1. Befestigen Sie eine Rackhalterung an einer Seite des EMX-Geräts.
   a. Richten Sie zwei ovalen Öffnungen der Rackhalterung mit den beiden Gewindebohrungen an der Seite des EMX-Geräts aus.
   b. Sichern Sie die Rackhalterung mit den beiden von Raritan bereitgestellten Schrauben.

Hinweis: Die geeigneten Positionen der ovalen Öffnungen der Rackhalterung kann je nach den Gewindebohrungen Ihres Modells variieren.

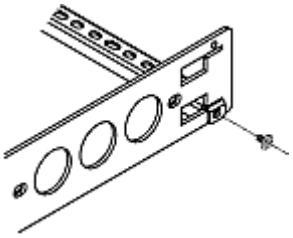


2. Wiederholen Sie Schritt 1, um die andere Rackhalterung an der anderen Seite des EMX-Geräts zu befestigen.

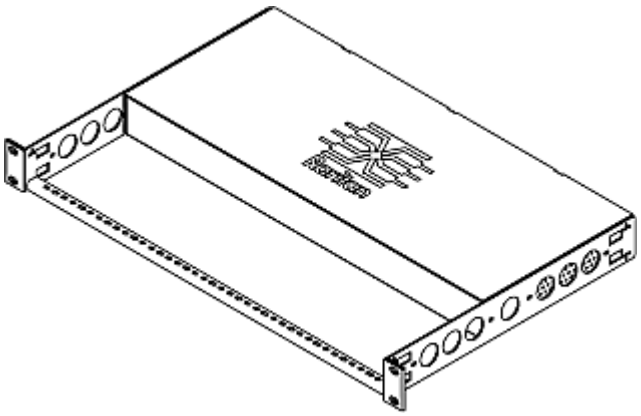
3. Führen Sie ein Ende der Kabelhalterungsleiste in die L-förmige Öffnung der Rackhalterung und richten Sie die Öffnung am Ende der Leiste mit der Gewindebohrung neben der L-förmigen Öffnung aus.



4. Sichern Sie die Kabelhalterungsleiste mit einer der von Raritan bereitgestellten Sechskantschrauben.



5. Wiederholen Sie die Schritte 3 bis 4, um das andere Ende der Kabelhalterungsleiste an der anderen Rackhalterung zu befestigen.



6. Montieren Sie das EMX-Gerät auf dem Rack, indem Sie die Ösen der Rackhalterung mit Ihren eigenen Schrauben, Bolzen, Käfigmuttern oder ähnlichem an den vorderen Schienen des Racks befestigen.

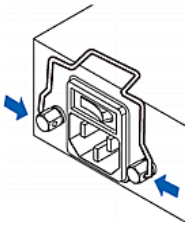
Anschließen der EMX-Einheit an eine Stromquelle

Wenn für das EMX-Gerät eine Kabelhaltefeder verwendet werden kann, bringen Sie die Feder an, bevor Sie das Netzkabel anschließen. Eine Kabelhaltefeder verhindert, dass sich das angeschlossene Netzkabel löst.

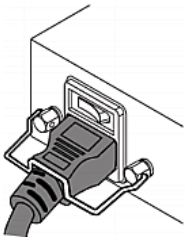
Die Verwendung von Kabelhaltefedern wird für Regionen mit hoher seismischer Aktivität und Umgebungen, in denen Erschütterungen und Vibrationen zu erwarten sind, empfohlen.

So schließen Sie das EMX-Gerät an eine Stromquelle an:

1. Befestigen Sie die Kabelhaltefeder, indem Sie die beiden Enden in die kleinen Öffnungen an den zwei Sechskantschrauben nahe der Anschlussbuchsen stecken.



2. Schließen Sie das eine Ende des von Raritan gelieferten Netzkabels an der Anschlussbuchse an, und drücken Sie Kabelhaltefeder in Richtung Netzkabel, bis das Kabel mithilfe der Feder fest sitzt.



3. Schließen Sie das andere Ende des Netzkabels an eine geeignete Stromquelle an.

Konfigurieren der EMX-Einheit

So konfigurieren Sie das EMX-Gerät:

1. Schließen Sie einen Computer über eine serielle oder eine USB-Verbindung an das EMX-Gerät an.
2. Schließen Sie das EMX-Gerät über eine drahtgebundene oder drahtlose Verbindung an das Netzwerk an.
3. Konfigurieren Sie das EMX-Gerät mithilfe der Befehlszeilenschnittstelle.

Anschließen der EMX-Einheit an einen Computer

Zum Konfigurieren der EMX-Einheit mit einem Computer muss die Einheit über eine serielle RS-232-Schnittstelle an einen Computer angeschlossen werden. Auf dem Computer muss ein Kommunikationsprogramm, wie z. B. HyperTerminal oder PuTTY, installiert sein.

Wenn Ihr Computer keinen seriellen Port hat, können Sie ein gewöhnliches USB-Kabel verwenden, um die EMX-Einheit zur Erstkonfiguration an den Computer anzuschließen. Das EMX-Gerät kann einen USB-Seriell-Adapter emulieren, nachdem der USB-Seriell-Treiber ordnungsgemäß unter Windows® installiert wurde.

Hinweis: Nicht alle Seriell-USB-Adapter funktionieren mit dem EMX-Gerät. Dieser Abschnitt bietet daher keine Einführung in die Verwendung solcher Adapter.

Schließen Sie die EMX-Einheit nun zur Erstkonfiguration anhand einer der folgenden Anweisungen an.

So erstellen Sie eine serielle Verbindung:

1. Schließen Sie ein Ende des Nullmodemkabels an den RS-232-Port mit der Bezeichnung CONSOLE / MODEM am EMX-Gerät an.
2. Schließen Sie das andere Ende des Nullmodemkabels an den seriellen Port (COM) des Computers an.

So erstellen Sie eine USB-Verbindung:

1. Schließen Sie ein Ende eines regulären USB-Kabels an den USB-B-Port am EMX-Gerät an.
2. Schließen Sie das andere Ende des USB-Kabels an den USB-A-Port des Computers an.

Installieren des USB-Seriell-Treibers

Die EMX-Einheit kann einen USB-Seriell-Adapter über eine USB-Verbindung emulieren. Für Microsoft® Windows®-Betriebssysteme ist ein USB-Seriell-Treiber mit dem Namen "Dominion Serial Console" erforderlich. Laden Sie die Treiberdatei *dominion-serial.zip*, die die Dateien *dominion-serial.inf* und *dominion-serial-setup.exe* enthält, von der ***Raritan-Website http://www.raritan.com*** unter ***Firmware and Documentation http://www.***, ***http://www.raritan.com/support/firmware-and-documentation/*** (Firmware und Dokumentation) für die EMX-Einheit herunter.

So installieren Sie den Treiber unter Windows® Vista und 7:

1. Ziehen Sie das USB-Kabel der EMX-Einheit vom Computer ab.
2. Führen Sie die Datei "dominion-serial-setup.exe" aus. Der Dominion Serial Console Driver Setup Wizard (Konfigurationsassistent für Treiber der seriellen Dominion-Konsole) wird aufgerufen.
3. Klicken Sie auf "Install" (Installieren), um den Treiber zu installieren.
4. Klicken Sie auf "Finish" (Fertig stellen), wenn die Installation abgeschlossen ist.
5. Schließen Sie das USB-Kabel der EMX-Einheit am Computer an. Der Treiber wird automatisch installiert.

So installieren Sie den Treiber unter Windows® XP:

1. Ziehen Sie das USB-Kabel der EMX-Einheit vom Computer ab.
2. Prüfen Sie, ob die Datei "usbser.sys" im Verzeichnis "C:\Windows\ServicePackFiles\i386" enthalten ist. Falls nicht, extrahieren Sie sie von der Windows-Installations-CD, und kopieren Sie sie in das Verzeichnis, in dem sich der USB-Seriell-Treiber befindet.
   - Auf einer CD mit SP3 müssen Sie die Datei aus I386\SP3.CAB extrahieren.
   - Auf einer CD mit SP2 müssen Sie die Datei aus I386\SP2.CAB extrahieren.
   - Auf einer CD ohne SP müssen Sie die Datei aus I386\DRIVER.CAB extrahieren.
3. Schließen Sie das USB-Kabel der EMX-Einheit am Computer an.
4. Der Computer erkennt das neue Gerät, und das Dialogfeld "Assistent für das Suchen neuer Hardware" wird angezeigt. Wenn dieses Dialogfeld nicht angezeigt wird, wählen Sie "Systemsteuerung > System > Hardware > Geräte-Manager", klicken Sie mit der rechten Maustaste auf "Dominion Serial Console" (Serielle Dominion-Konsole), und wählen Sie "Update Driver" (Treiber aktualisieren).

5. Wählen Sie "Install from a list or specific location" (Software von einer Liste oder bestimmten Quelle installieren) aus, und geben Sie den Speicherort des Treibers ein.
6. Wenn Sie nach der Datei "usbser.sys" gefragt werden, geben Sie den Speicherort der Datei an.
7. Die Installation ist abgeschlossen.

Unter Linux:

Es sind keine zusätzlichen Treiber erforderlich, Sie müssen jedoch den Namen des TTY-Geräts angeben. Sie finden diesen in der Ausgabe von "dmesg", nachdem Sie das EMX-Gerät an den Computer angeschlossen haben. In der Regel lautet der Name des TTY-Geräts "/dev/ttyACM#" oder "/dev/ttyUSB#", wobei # für eine ganze Zahl steht.

Führen Sie z. B. die folgenden Befehle aus, wenn Sie das Terminalprogramm Kermit verwenden und das TTY-Gerät "/dev/ttyACM0" ist:

> set line /dev/ttyACM0

> connect

Anschließen der EMX-Einheit an das Netzwerk

Um die EMX-Einheit über die Webschnittstelle zu verwalten, müssen Sie die EMX-Einheit mit dem lokalen Netzwerk (LAN) verbinden. Die EMX-Einheit kann an ein drahtgebundenes oder drahtloses Netzwerk angeschlossen werden.

So erstellen Sie eine drahtgebundene Verbindung:

1. Schließen Sie ein UTP-Standardkabel der Kategorie 5e/6 an den ETHERNET-Port der EMX-Einheit an.
2. Verbinden Sie das andere Kabelende mit dem Netzwerk.

So erstellen Sie eine drahtlose Verbindung:

Führen Sie einen der folgenden Schritte durch:

- Schließen Sie einen 802.11n Wireless USB LAN-Adapter an den USB-A-Port an Ihrer EMX-Einheit an.
- Schließen Sie eine USB-Dockingstation an den USB-A-Port an der EMX-Einheit an, und schließen Sie den 802.11n Wireless USB LAN-Adapter an den entsprechenden USB-Port der Dockingstation an.

Unterstützte Wireless-LAN-Konfiguration

Wenn Sie die drahtlose Verbindung wählen, stellen Sie sicher, dass Ihr Wireless USB LAN-Adapter und Ihre Drahtlosnetzwerkkonfiguration die folgenden Anforderungen erfüllen.

- Netzwerk-Typ: 802.11n
- Protokoll: WPA2 (RSN)
- Schlüsselverwaltung: WPA-PSK
- Verschlüsselung: CCMP (AES)

Wichtig: Momentan werden nur von Raritan bereitgestellte Wireless USB LAN-Adapter unterstützt. Sie können den technischen Support von Raritan kontaktieren, um diese Informationen zu erhalten.

Erstkonfiguration des Netzwerks

Sobald das EMX-Gerät mit dem Netzwerk verbunden ist, müssen Sie eine IP-Adresse und einige weitere Netzwerkinformationen konfigurieren.

In diesem Abschnitt wird die Erstkonfiguration über eine serielle oder eine USB-Verbindung beschrieben. Informationen zum Konfigurieren der EMX-Einheit über das LAN finden Sie unter ***Ändern der Netzwerkkonfiguration (BCM, EMX, PX2, PXE)*** (siehe "***Ändern der Netzwerkkonfiguration***" auf Seite 81).

So konfigurieren Sie das EMX-Gerät:

1. Öffnen Sie auf dem Computer, an dem Sie die EMX-Einheit angeschlossen haben, ein Kommunikationsprogramm, wie z. B. HyperTerminal oder PuTTY.
2. Wählen Sie den entsprechenden COM-Port aus, und vergewissern Sie sich, dass die Porteinstellungen wie folgt konfiguriert sind:
   - Bits per second (Bits pro Sekunde) = 115200 (115,2 Kbit/s)
   - Data bits (Datenbits) = 8
   - Stop bits (Stoppbits) = 1
   - Parity (Parität) = None (Keine)
   - Flow control (Flusssteuerung) = None (Keine)

   Tipp: Bei einer USB-Verbindung können Sie feststellen, welcher COM-Port der EMX-Einheit zugeordnet ist. Wählen Sie dazu "Control Panel" (Systemsteuerung) > "System" > "Hardware" > "Device Manager" (Geräte-Manager)", und suchen Sie "Dominion Serial Console" (Serielle Dominion-Konsole) in der Gruppe "Ports".
3. Drücken Sie die Eingabetaste.

4. Die EMX-Einheit fordert Sie zur Anmeldung auf. Beachten Sie beim Benutzernamen und Kennwort die Groß-/Kleinschreibung.
   a. Geben Sie bei der Eingabeaufforderung "Username" (Benutzername) `admin` ein, und drücken Sie die Eingabetaste.
   b. Geben Sie bei der Eingabeaufforderung "Password" (Kennwort) `raritan` ein, und drücken Sie die Eingabetaste.
5. Sie werden aufgefordert, das Kennwort zu ändern, wenn Sie sich zum ersten Mal bei der EMX-Einheit anmelden. Befolgen Sie die Anweisungen auf dem Bildschirm, um das neue Kennwort einzugeben.
6. Die Eingabeaufforderung # wird angezeigt, nachdem Sie sich erfolgreich angemeldet haben.
7. Geben Sie `config` ein, und drücken Sie die Eingabetaste.
8. Um die Netzwerkeinstellungen zu konfigurieren, geben Sie die entsprechenden Befehle ein und drücken die Eingabetaste. Bei allen Befehlen ist die Groß-/Kleinschreibung zu beachten.
   a. Mit dem folgenden Befehl stellen Sie den Netzwerkmodus ein:

      `network mode <mode>`

      dabei ist <mode> (Modus) entweder *wired* (drahtgebunden) für eine drahtgebundene Verbindung (Standard) oder *wireless* (drahtlos) für eine drahtlose Verbindung.
   b. Für den drahtgebundenen Netzwerkmodus können Sie die Einstellungen der LAN-Schnittstelle konfigurieren. Für die meisten Szenarien funktioniert die Standardeinstellung "auto" (automatisch) und sie sollte nur geändert werden, wenn dies erforderlich ist.

Einstellen	Befehl
LAN interface speed (LAN-Schnittstellengeschwindigkeit)	`network interface LANInterfaceSpeed <option>` wobei <option> (Option) *auto* (automatisch), *10Mbps* 10Mbit/s oder *100Mbps* (100Mbit/s) sein kann.
LAN interface duplex mode (Duplex-Modus der LAN-Schnittstelle)	`network interface LANInterfaceDuplexMode <mode>` wobei <mode> (Modus) *half* (halb), *full* (voll) oder *auto* (automatisch) sein kann.

Tipp: Sie können mehrere Befehle kombinieren, um mehrere Parameter gleichzeitig zu konfigurieren. Beispiel:
`network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

c. Für den Drahtlosnetzwerkmodus müssen Sie die Service Set Identifier (SSID)-Parameter konfigurieren.

Einstellen	Befehl
SSID	`network wireless SSID <ssid>` Dabei steht <ssid> für den SSID-String.

Konfigurieren Sie bei Bedarf weitere Drahtlosparameter, die in der folgenden Tabelle dargestellt sind.

Einstellen	Befehl
BSSID	`network wireless BSSID <bssid>` Dabei ist <bssid> die AP-MAC-Adresse.
Authentication method (Authentifizierungsmethode)	`network wireless authMethod <method>` Dabei ist <method> (Methode) *psk* für "Pre-Shared Key" (vorher vereinbarter Schlüssel) oder *eap* für "Extensible Authentication Protocol" (Erweiterbares Authentifizierungsprotokoll).
PSK	`network wireless PSK <psk>` Dabei steht <psk> für den PSK-String.
EAP outer authentication (EAP äußere Authentifizierung)	`network wireless eapOuterAuthentication <outer_auth>` Dabei ist <outer_auth> *PEAP*.
EAP inner authentication (EAP innere Authentifizierung)	`network wireless eapInnerAuthentication <inner_auth>` Dabei ist <inner_auth> *MSCHAPv2*.

Einstellen	Befehl
EAP identity (EAP-Identität)	`network wireless eapIdentity <identity>` Dabei ist <identity> (Identität) Ihr Benutzername für die EAP-Authentifizierung.
EAP password (EAP-Kennwort)	`network wireless eapPassword` Geben Sie das Kennwort für die EAP-Authentifizierung ein, wenn Sie dazu aufgefordert werden.
EAP CA certificate (EAP-CA-Zertifikat)	`network wireless eapCACertificate` Öffnen Sie bei der Aufforderung zur Eingabe des CA-Zertifikats das Zertifikat mit einem Textbearbeitungsprogramm, kopieren Sie den Inhalt und fügen Sie diesen in das Kommunikationsprogramm ein.

Hinweis: Der zu kopierende Inhalt des CA-Zertifikats umfasst NICHT die erste Zeile "BEGIN CERTIFICATE" und die letzte Zeile "END CERTIFICATE."

d. Um festzustellen, welches IP-Protokoll aktiviert und welche vom DNS-Server zurückgegebene IP-Adresse verwendet wird, konfigurieren Sie die folgenden Parameter.

Einstellen	Befehl
IP protocol (IP-Protokoll)	`network ip proto <protocol>` Dabei ist <protocol> (Protokoll) *v4Only* zur Aktivierung von IPv4, *v6Only* zur Aktivierung von IPv6 oder *both* (Beides) zur Aktivierung von IPv4- und IPv6-Protokollen.
Vom DNS-Server zurückgegebene IP-Adresse	`network ip dnsResolverPreference <resolver>` Dabei ist <resolver> (Resolver) *preferV4* für IPv4-Adressen oder *preferV6* für IPv6-Adressen.

e. Wenn Sie im vorhergehenden Schritt das IPv4-Protokoll aktiviert haben, konfigurieren Sie die IPv4-Netzwerkparameter.

Einstellen	Befehl
IP configuration method (IP-Konfigurationsmethode)	`network ipv4 ipConfigurationMode <mode>` Dabei steht <Modus> für *dhcp* für die automatische Konfiguration (Standard) oder für *static* (statisch) zum Angeben einer statischen IP-Adresse ist.

- Konfigurieren Sie für die IPv4-DHCP-Konfiguration diesen Parameter.

Einstellen	Befehl
Bevorzugter Hostname (optional)	`network ipv4 preferredHostName <name>` Dabei steht <Name> für den bevorzugten Hostnamen.

Tipp: Um die DHCP-zugewiesenen IPv4-DNS-Server mit den von Ihnen manuell eingegeben zu überschreiben, geben Sie diesen Befehl ein:

`network ipv4 overrideDNS <option>`

Dabei ist <option> (Option) `enable` (aktivieren) oder `disable` (deaktivieren). Die IPv4-Befehle zur manuellen Angabe der DNS-Server finden Sie in der folgenden Tabelle.

- Konfigurieren Sie für die statische IPv4-Konfiguration diese Parameter.

Einstellen	Befehl
Static IPv4 address (Statische IPv4-Adresse)	`network ipv4 ipAddress <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse, die Sie zuweisen möchten.

Einstellen	Befehl
Subnetzmaske	`network ipv4 subnetMask <netmask>` Dabei steht <Netzmaske> für die Subnetzmaske.
Gateway	`network ipv4 gateway <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des Gateways.
Primärer DNS-Server	`network ipv4 primaryDNSServer <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des primären DNS-Servers.
Sekundärer DNS-Server (optional)	`network ipv4 secondaryDNSServer <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des sekundären DNS-Servers.

f. Wenn Sie im vorhergehenden Schritt IPv6 aktiviert haben, konfigurieren Sie die IPv6-Netzwerkparameter.

Einstellen	Befehl
IP configuration method (IP-Konfigurationsmethode)	`network ipv6 ipConfigurationMode <mode>` Dabei ist <mode> (Modus) entweder *automatic* für die automatische Konfiguration (Standard) oder *static* (statisch) zum Angeben einer statischen IP-Adresse.

Tipp: Um die DHCP-zugewiesenen IPv6-DNS-Server mit den von Ihnen manuell eingegeben zu überschreiben, geben Sie diesen Befehl ein:

`network ipv6 overrideDNS <option>`

Dabei ist <option> (Option) `enable` (aktivieren) oder `disable` (deaktivieren). Die IPv6-Befehle zur manuellen Angabe der DNS-Server finden Sie in der folgenden Tabelle.

- Konfigurieren Sie für die statische IPv6-Konfiguration die folgenden Parameter. Beachten Sie, dass die IP-Adresse dem IPv6-Format entsprechen muss.

Einstellen	Befehl
Static IPv6 address (Statische IPv6-Adresse)	`network ipv6 ipAddress <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse, die Sie zuweisen möchten.
Gateway	`network ipv6 gateway <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des Gateways.
Primärer DNS-Server	`network ipv6 primaryDNSServer <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des primären DNS-Servers.
Sekundärer DNS-Server (optional)	`network ipv6 secondaryDNSServer <ip address>` Dabei steht <IP-Adresse> für die IP-Adresse des sekundären DNS-Servers.

9. Um den Konfigurationsmodus mit oder ohne Speichern der Änderungen zu beenden, geben Sie den entsprechenden Befehl ein und drücken die Eingabetaste.

Befehl	Beschreibung
`apply (Übernehmen)`	Alle Konfigurationsänderungen speichern und den Konfigurationsmodus beenden.
`cancel (Abbrechen)`	Alle Konfigurationsänderungen verwerfen und den Konfigurationsmodus beenden.

Die Eingabeaufforderung # wird angezeigt und weist darauf hin, dass Sie den Konfigurationsmodus beendet haben.

10. Um die Richtigkeit aller Einstellungen zu überprüfen, geben Sie die folgenden Befehle nacheinander ein. Die aktuellen Netzwerkeinstellungen werden angezeigt.

Befehl	Beschreibung
`show network`	Zeigt Netzwerkparameter an.
`show network ip` alle	Zeigt alle IP-Konfigurationsparameter an.
`show network wireless details`	Zeigt alle Wireless-Parameter an. (Führen Sie diesen Befehl nur aus, wenn Sie den drahtlosen Modus aktivieren.)

Tipp: Sie können auch "`show network wireless`" eingeben, um eine verkürzte Version der drahtlosen Einstellungen anzuzeigen.

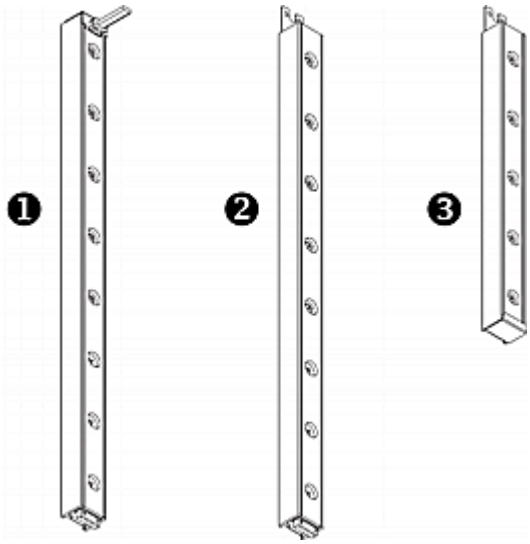
11. Wenn alle Einstellungen korrekt sind, geben Sie `exit` ein, um sich bei der EMX-Einheit abzumelden. Wenn eine Einstellung falsch ist, wiederholen Sie die Schritte 7 bis 10, um die Netzwerkeinstellungen zu ändern.

Es kann einige Sekunden dauern, bis die konfigurierte IP-Adresse wirksam wird.

Verknüpfen von Assetsensoren

Jeder Tag-Port an den Asset-Sensoren entspricht einer Rackeinheit und kann verwendet werden, um die Position von IT-Geräten auf einem bestimmten Rack (oder Schrank) zu ermitteln. Für jedes Rack können bis zu 64U-Asset-Sensoren angeschlossen werden, die aus einem MASTER- und mehreren SLAVE-Asset-Sensoren bestehen. Der Unterschied zwischen dem Master-Asset-Sensor und den Slave-Asset-Sensoren besteht darin, dass der Master-Asset-Sensor im Gegensatz zu den Slave-Asset-Sensoren über einen RJ-45-Anschluss verfügt.

Die folgende Abbildung zeigt Asset-Sensoren. Die Abbildung zeigt nicht alle Typen von Asset-Sensoren, die von Raritan angeboten werden.

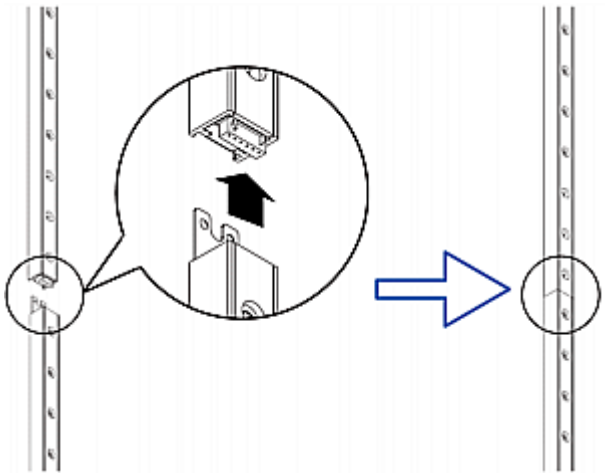


Nummer	Position
❶	8U-MASTER-Asset-Sensor mit 8 Tag-Ports
❷	8U-SLAVE-Asset-Sensor mit 8 Tag-Ports
❸	5U-"Abschluss"-SLAVE-Asset-Sensor mit 5 Tag-Ports

Hinweis: Im Gegensatz zu normalen Slave-Asset-Sensoren, die einen DIN-Stecker an jedem Ende haben, verfügt der Abschluss-Slave-Asset-Sensor lediglich an einem Ende einen DIN-Stecker. Ein Abschluss-Asset-Sensor wird am Ende der Asset-Sensor-Baugruppe installiert.

So montieren Sie Asset-Sensoren:

1. Schließen Sie einen MASTER-Asset-Sensor an einen 8U-SLAVE-Asset-Sensor an.
   - Stecken Sie den weißen DIN-Stecker des Slave-Asset-Sensors in die weiße DIN-Buchse des Master-Asset-Sensors.
   - Stellen Sie sicher, dass das U-förmige Blech neben dem DIN-Stecker in den hinteren Slot des Master-Asset-Sensors gesteckt wird. Verschrauben Sie das U-förmige Blech, um die Verbindung zu verstärken.



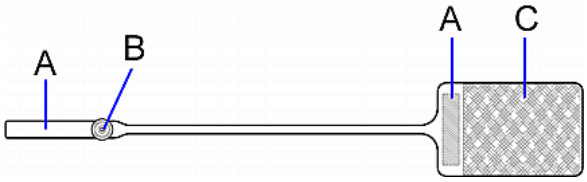
2. Schließen Sie auf die selbe Weise wie in Schritt 1 einen weiteren 8U-Slave-Asset-Sensor an den Sensor an, der am Master-Asset-Sensor befestigt ist.
3. Wiederholen Sie den oben beschriebenen Schritt, um weitere Slave-Asset-Sensoren anzuschließen. Die Asset-Sensor-Baugruppe darf bis zu 64U lang sein.
   - Der letzte Asset-Sensor kann 8U oder 5U sein, je nach der tatsächlichen Höhe Ihres Racks.
   - Es empfiehlt sich dringend, den "Abschluss"-Asset-Sensor als letzten Asset-Sensor zu verwenden.
4. Befestigen Sie die Asset-Sensor-Baugruppe neben den IT-Geräten vertikal am Rack, sodass jeder Tag-Port horizontal mit einer Rackeinheit ausgerichtet ist. Die Asset-Sensoren werden von dem Rack automatisch gehalten, da sich an der Rückseite Magnetstreifen befinden.

Hinweis: Der Asset-Sensor verfügt über einen Neigungssensor, sodass der Asset-Sensor umgekehrt montiert werden kann.

Anschließen von Assetsensoren an das EMX-Gerät

Sie benötigen Asset-Sensoren und Asset-Tags zur Verfolgung von IT-Geräten. Asset-Tags, die sich an IT-Geräten befinden, stellen eine ID-Nummer für jedes IT-Gerät bereit, während die Assetsensoren Informationen zu ID-Nummern und Position an das angeschlossene EMX-Gerät übertragen.

Die folgende Abbildung zeigt ein Asset-Tag.



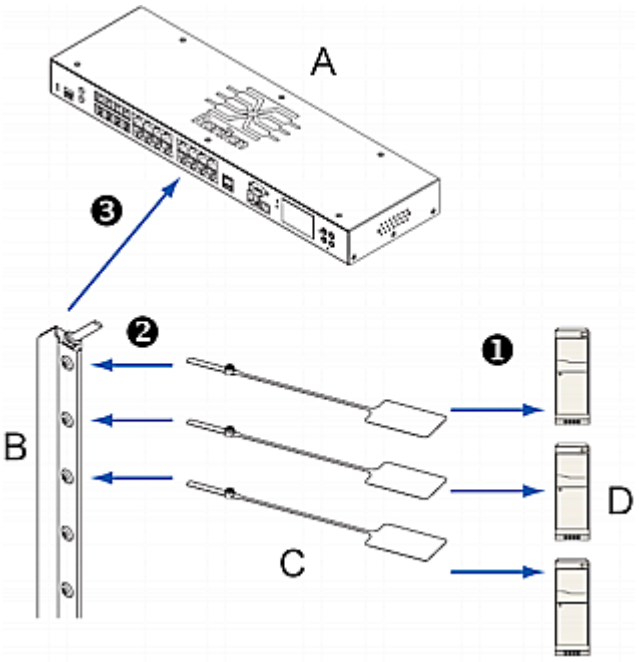
Buchstabe	Position
A	Strichcode (ID-Nummer), die an beiden Enden des Asset-Tags verfügbar ist
B	Tag-Stecker
C	Klebebereich mit Band

Hinweis: Der Strichcode jedes Asset-Tags ist eindeutig und wird in der EMX-Webschnittstelle angezeigt, sodass es leicht identifiziert werden kann.

So schließen Sie Asset-Sensoren an das EMX-Gerät an:

1. Befestigen Sie das klebende Ende eines Asset-Tags an jedem IT-Gerät.
2. Stecken Sie den Stecker am anderen Ende jedes Asset-Tags in den entsprechenden Tag-Port am Asset-Sensor.
3. Schließen Sie die Asset-Sensor-Baugruppe am Rack wie folgt an das EMX-Gerät an:
   a. Schließen Sie ein Ende des Kabels der Kategorie 5e/6 an den RJ-45-Stecker am MASTER-Asset-Sensor an.
   b. Schließen Sie das andere Ende des Kabels an den FEATURE-Port auf dem EMX-Gerät an.

Das EMX-Gerät versorgt die Asset-Sensor-Baugruppe über das Kabel der Kategorie 5e/6 mit Strom. Alle LEDs der Asset-Sensor-Baugruppe leuchten beim Einschalten abwechselnd in verschiedenen Farben, wenn die Firmware des Asset-Sensors vom EMX-Gerät aktualisiert wird. Nach dem Einschalten oder nach Abschluss des Firmware-Upgrades leuchten die LEDs permanent in einer Farbe. Die LED-Farbe der Tag-Ports mit angeschlossenen Asset-Tags unterscheidet sich von der LED-Farbe der Tag-Ports ohne angeschlossene Asset-Tags.



Modell

Buchstabe	Position
A	EMX-Gerät
B	Asset-Sensoren
C	Asset-Tags
D	IT-Geräte, z. B. Server

EMX2-111 unterstützt eine Kabellänge von maximal 1-m für den Anschluss der Assetsensor-Baugruppe, während Modell EMX2-888 eine Kabellänge von maximal 10-m für den Anschluss jeder Assetsensor-Baugruppe unterstützt.

4. Wenn das Gerät über mehrere FEATURE-Ports verfügt, wiederholen Sie die oben beschriebenen Schritte, um weitere Assetsensoren an die restlichen FEATURE-Ports anzuschließen.

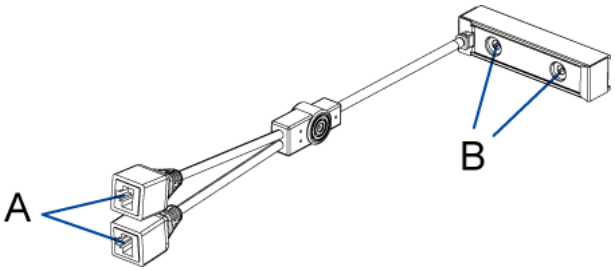
5. Konfigurieren Sie die Assetsensoren. Siehe ***Konfigurieren des Asset-Sensors*** (siehe "***Konfigurieren des Assetsensors***" auf Seite 191).

Anschließen von AMS-M2-Z-Assetsensoren (optional)

Der AMS-M2-Z ist ein besonderer Typ eines Assetsensors, der – mit dem folgenden Unterschied – wie normale MASTER-Assetsensoren funktioniert.

- Er stellt zwei RJ-45-Anschlüsse bereit.
- Es besteht die Möglichkeit, mehrere AMS-M2-Z-Assetsensoren zu verketten.
- An jedem AMS-M2-Z sind nur zwei Tag-Ports verfügbar, sodass nur zwei Asset-Tags angeschlossen werden können.

Dieses Produkt eignet sich besonders zum Überwachen großer Geräte wie SAN-Boxes im Schrank.

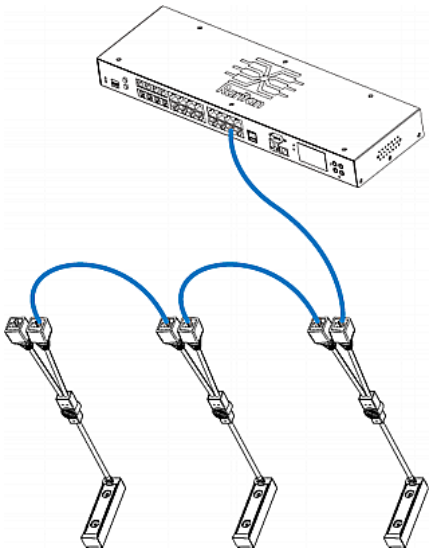


Position	Beschreibung
A	RJ-45-Anschlüsse
B	Tag-Ports

So schließen Sie AMS-M2-Z-Assetsensoren an die EMX-Einheit an:

1. Schließen Sie den AMS-M2-Z über ein Kabel der Kategorie 5e/6 an die EMX-Einheit an.
   a. Schließen Sie ein Ende des Kabels an den RJ-45-Port mit der Beschriftung "Input" (Eingang) am AMS-M2-Z an.
   b. Schließen Sie das andere Ende des Kabels an den FEATURE-Port der EMX-Einheit an.
2. Befestigen Sie das Asset-Tag am IT-Gerät, und schließen Sie das Asset-Tag am AMS-M2-Z an, indem Sie den Tag-Stecker mit dem Tag-Port am AMS-M2-Z verbinden. Weitere Informationen finden Sie unter ***Anschließen von Asset-Sensoren an das EMX-Gerät*** (siehe "***Anschließen von Assetsensoren an das EMX-Gerät***" auf Seite 24).

3. Falls erforderlich, verketten Sie mehrere AMS-M2-Z, um mehr als zwei IT-Geräte über diese EMX-Einheit zu verfolgen.
   a. Prüfen Sie, ob die Länge des Kabels der Kategorie 5e/6 innerhalb der Grenzen liegt. Informationen zu Einschränkungen bei der Kabellänge finden Sie unter ***Einschränkungen beim Verketten von AMS-M2-Z-Sensoren*** (auf Seite 197).
   b. Verbinden Sie ein Ende des Kabels der Kategorie 5e/6 mit dem RJ-45-Anschluss mit der Beschriftung "Output" (Ausgang) des AMS-M2-Z, der an die EMX-Einheit angeschlossen wird.
   c. Schließen Sie das andere Ende des Kabels an den RJ-45-Anschluss mit der Beschriftung "Input" (Eingang) an einem anderen AMS-M2-Z an.
   d. Wiederholen Sie die oben beschriebenen Schritte, um weitere AMS-M2-Z-Sensoren zu verketten. Informationen zur maximalen Anzahl an AMS-M2-Z-Assetsensoren, die verkettet werden können, finden Sie unter ***Einschränkungen beim Verketten von AMS-M2-Z-Sensoren*** (auf Seite 197).
   e. Um das Gewicht aller Verbindungskabel halten zu können, empfiehlt es sich dringend, die Kabelbinder zu verwenden.



4. Wiederholen Sie Schritt 2, um IT-Geräte über die Asset-Tags an die anderen AMS-M2-Z-Sensoren in der Reihe anzuschließen.

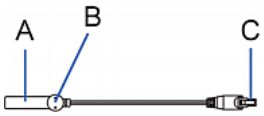
Anschließen von Blade-Erweiterungsstrips

Bei Blade-Servern, die in einem einzigen Gehäuse untergebracht sind, können Sie einzelne Blade-Server über einen Blade-Erweiterungsstrip verfolgen.

Der Blade-Erweiterungsstrip von Raritan funktioniert ähnlich dem Raritan-Assetsensor, benötigt aber ein Tag-Anschlusskabel für den Anschluss an einen Tag-Port am regulären Assetsensor oder AMS-M2-Z. Der Blade-Erweiterungsstrip enthält je nach Modell 4 bis 16 Tag-Ports.

Die Abbildung zeigt ein Tag-Anschlusskabel und einen Blade-Erweiterungsstrip mit 16 Tag-Ports.

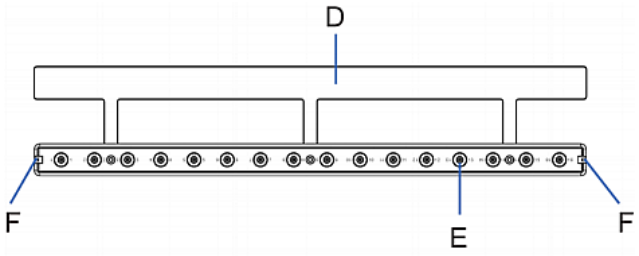
Tag-Anschlusskabel



Position	Beschreibung
A	Strichcode (ID-Nummer) für das Tag-Anschlusskabel
B	Tag-Stecker
C	Kabelanschluss zum Anschließen des Blade-Erweiterungsstrips

Hinweis: Ein Tag-Anschlusskabel hat einen eindeutigen Strichcode. Dieser wird in der EMX-Webschnittstelle zur Identifikation jedes Blade-Erweiterungsstrips angezeigt, an den es angeschlossen ist.

Blade-Erweiterungsstrip



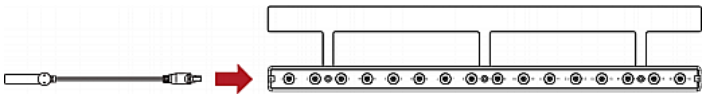
Position	Beschreibung
D	Mylar-Bereich mit Klebeband
E	Tag-Ports

Position	Beschreibung
F	Kabelbuchse(n) zum Anschließen des Tag-Anschlusskabels

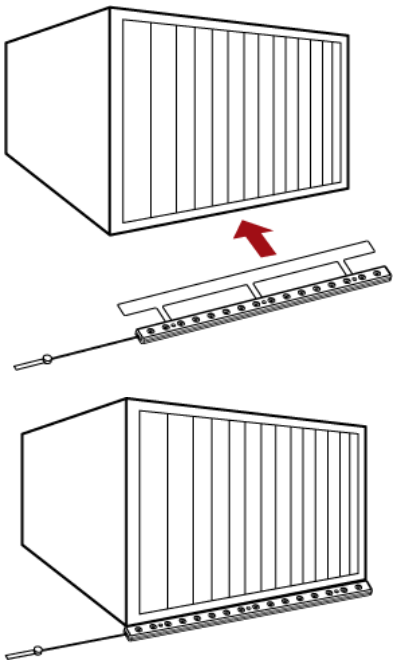
Hinweis: Jeder Tag-Port auf dem Blade-Erweiterungsstrip ist mit einer Nummer versehen, die als Slot-Nummer in der EMX-Webschnittstelle angezeigt wird.

So installieren Sie einen Blade-Erweiterungsstrip:

1. Schließen Sie das Tag-Anschlusskabel an den Blade-Erweiterungsstrip an.
   - Stecken Sie den Stecker des Kabels in eine der beiden Buchsen des Blade-Erweiterungsstrips.



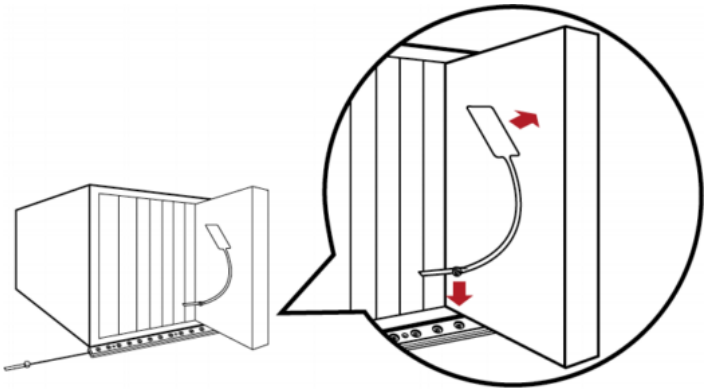
2. Schieben Sie den Blade-Erweiterungsstrip unter das Blade-Gehäuse, bis sich der Mylar-Bereich vollständig unter dem Gehäuse befindet. Vergewissern Sie sich, dass sich der Blade-Erweiterungsstrip nicht löst. Verwenden Sie ggf. das Klebeband an der Rückseite des Mylar-Bereichs, um den Strip zu fixieren.



3. Schließen Sie ein Ende des Asset-Tags an den Blade-Server und das andere Ende an den Blade-Erweiterungsstrip an.

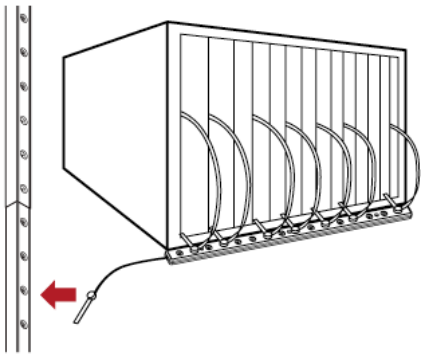
a. Befestigen Sie das Asset-Tag mit dem Klebeband des Tags an einer Seite des Blade-Servers.

b. Schließen Sie den Tag-Stecker des Asset-Tags am Tag-Port des Blade-Erweiterungsstrips an.



4. Wiederholen Sie den vorhergehenden Schritt, bis alle Blade-Server im Gehäuse über die Asset-Tags mit dem Blade-Erweiterungsstrip verbunden sind.

5. Schließen Sie den Tag-Stecker des Blade-Erweiterungsstrips am nächstgelegenen Tag-Port der Assetsensor-Baugruppe oder des AMS-M2-Z-Assetsensors am Rack an.



Hinweis: Wenn Sie den Tag-Stecker des Blade-Erweiterungsstrips vorübergehend abziehen müssen, warten Sie mindestens 1 Sekunde, bevor Sie ihn wieder anschließen, weil die EMX-Einheit ihn sonst nicht erkennt.

Anschließen der Umgebungssensoren (optional)

Um die Erkennung von Umgebungsfaktoren um die EMX-Einheit zu ermöglichen, schließen Sie mindestens einen Raritan-Umgebungssensor an die EMX-Einheit an.

Der maximale Abstand für alle an den Sensorport des Produkts angeschlossenen Sensorkabel darf 30 Meter nicht übersteigen. Wenden Sie sich an den technischen Kundendienst von Raritan, wenn Sie Fragen haben.

Wenn ein Raritan-Sensorhub verwendet wird, können Sie bis zu 16 Umgebungssensoren je SENSOR-Port anschließen. Das bedeutet Folgendes:

- Für Modell EMX2-111, das nur 1 SENSOR-Port besitzt, können maximal 16 Umgebungssensoren angeschlossen werden.
- Für Modell EMX2-888, das 8 SENSOR-Ports besitzt, können maximal 128 Umgebungssensoren angeschlossen werden. Da das EMX2-888-Gerät mit zwei Channels für integrierte Kontaktschluss-Anschlüsse implementiert ist, unterstützt es maximal 130 Umgebungssensoren.

Jeder SENSOR-Port kann nur maximal zwei Raritan-Kontaktschlusssensoren unterstützen, die das kürzeste Aktualisierungsintervall unter allen Raritan-Sensoren haben. Siehe ***Informationen zum Aktualisierungsintervall*** (auf Seite 183).

Raritan-Umgebungssensoren enthalten in der Regel mehrere Sensoren. So zählen ein DPX-T2H2 und ein DPX-T3H1 beispielsweise jeweils als 4 Sensoren.

Warnung: Für einen ordnungsgemäßen Betrieb warten Sie 15 bis 30 Sekunden zwischen jedem Anschließen und jedem Trennen von Umgebungssensoren.

So schließen Sie einen oder mehrere Umgebungssensoren direkt an:

- Schließen Sie den Stecker des Umgebungssensors an den SENSOR-Port des EMX-Geräts an.

Hinweis: Die Gesamtanzahl der SENSOR-Ports hängt vom Gerätemodell ab.

So schließen Sie Umgebungssensoren über einen optionalen PX-Sensorhub an:

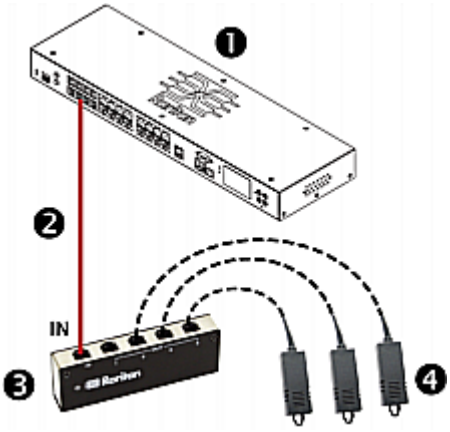
1. Schließen Sie einen Raritan-Sensorhub an das EMX-Gerät an.

a. Schließen Sie ein Ende des von Raritan mitgelieferten Telefonkabels (4 Drähte, 6 Pins, RJ-12) an den IN-Port (Port 1) des Hubs an.

b. Schließen Sie das andere Ende an einen der SENSOR-Ports am EMX-Gerät an.

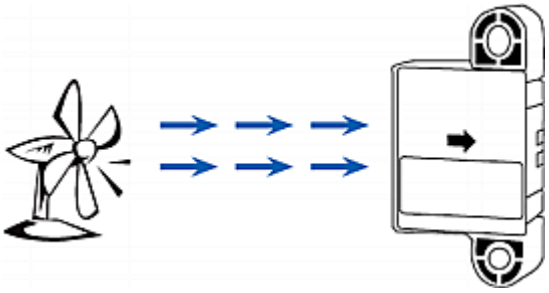
2. Schließen Sie die Raritan-Umgebungssensoren an einen beliebigen der vier OUT-Ports am Hub an.

   Raritan-Sensorhubs können NICHT hintereinandergeschaltet werden. Folglich kann maximal ein Sensorhub an jeden SENSOR-Port des EMX-Geräts angeschlossen werden. Die folgende Abbildung zeigt eine Konfiguration mit einem angeschlossenen Sensorhub.



❶	EMX-Gerät
❷	Von Raritan mitgeliefertes Telefonkabel
❸	Raritan PX-Sensorhub
❹	Raritan-Umgebungssensoren

3. Wenn Raritan-Luftstromsensoren angeschlossen sind, müssen Sie sicherstellen, dass sich der Sensor gegenüber der Luftquelle (z. B. einem Lüfter) in der richtigen Position befindet, die durch den Pfeil am Sensor gekennzeichnet ist.



4. Konfigurieren Sie den Umgebungssensor. Siehe ***Konfigurieren von Umgebungssensoren*** (auf Seite 177).

Informationen zu Kontaktschlusssensoren

Der Kontaktschlusssensor (DPX-CC2-TR) von Raritan kann den Offen-und-Geschlossen-Status der angeschlossenen Detektoren/Switches erkennen.

Damit dies ordnungsgemäß funktioniert, muss für dieses Feature mindestens ein Einzeldetektor/-switch (Ein/Aus) integriert sein. Es können unter anderem folgende Typen von Einzeldetektoren/-switches an den DPX-CC2-TR angeschlossen werden:

- Erkennung "Tür offen/geschlossen"
- Erkennung des Türschlossstatus
- Erkennung von Wasser
- Raucherkennung
- Erkennung von Erschütterungen

Raritan stellt keine Einzeldetektoren/-switches bereit. Es handelt sich dabei um Sensoren anderer Hersteller. Sie müssen sie in Verbindung mit dem DPX-CC2-TR von Raritan testen, um sicherzustellen, dass sie ordnungsgemäß arbeiten.

Wichtig: Für Integration und Test von Detektoren/Switches anderer Hersteller ist allein der Kunde verantwortlich. Raritan übernimmt keinerlei Haftung infolge eines ungeeigneten Anschlusses oder (beiläufig oder indirekt entstanden) Fehlers eines vom Kunden bereitgestellten und installierten Detektors/Switch eines anderen Herstellers. Eine Nichtbeachtung der Installations- und Konfigurationsanweisungen kann Fehlalarme oder keine Alarme zur Folge haben. Raritan macht keine Aussage darüber oder erhebt keinen Anspruch darauf, dass alle Detektoren/Switches anderer Hersteller in Verbindung mit dem DPX-CC2-TR funktionieren.

Anschluss von Detektoren/Switches anderer Hersteller

Detektoren/Switches anderer Hersteller lassen sich auf zwei Arten an das EMX-Gerät anschließen:

- Anschluss der Detektoren/Switches an den DPX-CC2-TR, der an einen SENSOR-Port des EMX-Geräts angeschlossen ist
- Anschluss der Detektoren/Switches an den Anschluss des Kontaktschlusssensors am EMX-Gerät, wenn das EMX-Gerät ein Modell EMX2-888 ist

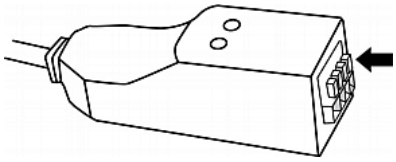
Anschluss von externen Detektoren/Switches an DPX-CC2-TR

Eine DPX-CC2-TR-Einheit bietet zwei Kanäle zum Anschluss von externen Detektoren/Switches. Es gibt vier federbelastete Anschlusspunkte am Gehäuse von DPX-CC2-TR: die beiden rechten sind mit einem Kanal verknüpft (durch die LED-Nummer angezeigt) und die beiden linken sind mit einem anderen Kanal verknüpft. Sie müssen die externen Detektoren/Switches in diese Anschlusspunkte stecken.

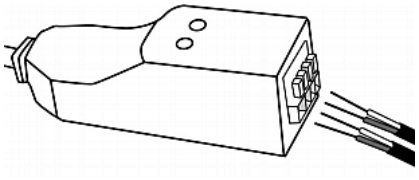
So schließen Sie externe Detektoren/Switches an:

1. Entfernen Sie die Isolierung bis etwa 12 mm vom Ende jedes Kabels bei zwei externen Detektoren/Switches.
2. Halten Sie die kleinen rechteckigen Knöpfe über den Anschlusspunkten am Gehäuse von DPX-CC2-TR nach unten gedrückt.

Hinweis: Jeder Knopf steuert die Feder des jeweiligen Anschlusspunktes.



3. Sie müssen jeden Draht der externen Detektoren/Switches in jeden Anschlusspunkt stecken.
   - Stecken Sie beide Drähte eines Detektors/Switch in die beiden Anschlusspunkte links.
   - Stecken Sie beide Drähte eines weiteren Detektors/Switch in die beiden Anschlusspunkte rechts.



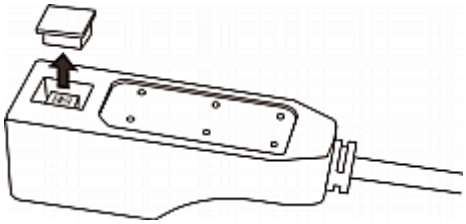
4. Lassen Sie die kleinen rechteckigen Knöpfe los, nachdem Sie die Drähte richtig eingesetzt haben.
5. Prüfen Sie, dass diese Drähte sicher befestigt sind.

Konfigurieren eines Kontaktschlusssensors

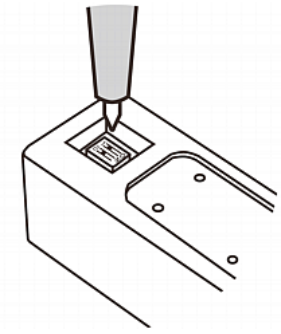
Bevor Sie den DPX-CC2-TR zur Erkennung des Kontaktschlussstatus, von Wasser, Rauch oder Erschütterungen verwenden, müssen Sie den Normalzustand festlegen. Stellen Sie dazu den DIP-Schalter, der den LED-Status steuert, am DPX-CC2-TR-Gehäuse ein. Ein DIP-Schalter ist einem Channel zugeordnet.

So passen Sie die Einstellung des DIP-Schalters an:

1. Platzieren Sie die an den DPX-CC2-TR angeschlossenen Detektoren/Switches an der Stelle, an der Sie eine bestimmte Umgebungssituation erkennen möchten.
2. Legen Sie den DIP-Schalter am DPX-CC2-TR-Gehäuse frei.



3. Um den Normalzustand für Channel 1 festzulegen, suchen Sie den DIP-Schalter mit der Kennzeichnung 1.
4. Bewegen Sie den Schiebeschalter mit einem spitzen Gegenstand wie einem Stift zu dem mit NO (Normally Open) oder NC (Normally Closed) gekennzeichneten Ende.
   - Normally Open (Normalerweise offen): Der Status "Offen" des angeschlossenen Detektors/Switch ist der Normalzustand.
   - Normally Closed (Normalerweise geschlossen): Der Status "Geschlossen" des angeschlossenen Detektors/Switch ist der Normalzustand. Dies ist die Standardeinstellung.



5. Um den Normalzustand für Channel 2 festzulegen, wiederholen Sie Schritt 4, um die Einstellung des anderen DIP-Schalters anzupassen.
6. Bringen Sie die Abdeckung des DIP-Schalters wieder an.

Hinweis: Die Einstellung des DIP-Schalters muss korrekt sein, andernfalls leuchtet die Sensor-LED fälschlicherweise im Normalzustand.

Anschluss von Detektoren/Switches anderer Hersteller an das EMX-Gerät

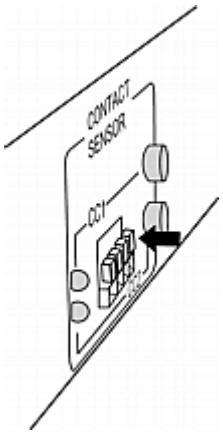
Das EMX-Modell EMX2-888 bietet zwei Channels für Kontaktschlusssensor-Anschlusspunkte, die den direkten Anschluss von Kontaktschluss-Detektoren/Switches anderer Hersteller ermöglichen.

Es kann nicht garantiert werden, dass alle Detektoren/Switches anderer Hersteller mit dem EMX-Gerät kompatibel sind. Sie müssen nach deren Installation einen Kompatibilitätstest durchführen.

So schließen Sie externe Detektoren/Switches an:

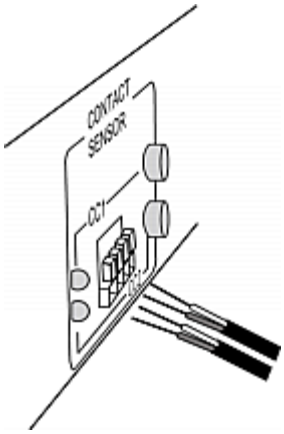
1. Entfernen Sie die Isolierung bis etwa 12 mm vom Ende jedes Kabels bei zwei externen Detektoren/Switches.
2. Drücken Sie die kleinen rechteckigen Knöpfe oberhalb der Anschlusspunkte, und halten Sie sie gedrückt.

   Hinweis: Jeder Knopf steuert die Feder des jeweiligen Anschlusspunktes.



3. Sie müssen jeden Draht der externen Detektoren/Switches in jeden Anschlusspunkt stecken.
   - Stecken Sie beide Drähte eines Detektors/Switch in die beiden Anschlusspunkte links.

- Stecken Sie beide Drähte eines weiteren Detektors/Switch in die beiden Anschlusspunkte rechts.



4. Lassen Sie die kleinen rechteckigen Knöpfe los, nachdem Sie die Drähte richtig eingesetzt haben.
5. Prüfen Sie, dass diese Drähte sicher befestigt sind.
6. Der Status "Offen" des Detektors/Switch ist standardmäßig der Normalzustand. Um die "normale" Einstellung auf "geschlossen" festzulegen, drücken Sie den entsprechenden Knopf nahe der Anschlusspunkte.

LEDs des Kontaktschlusssensors

In der Nähe der Kontaktschluss-Anschlusspunkte am EMX-Gerät oder am Kontaktschlusssensor-Modul (DPX-CC2-TR) von Raritan befinden sich zwei LEDs. Jede LED zeigt den Status des entsprechenden Channel.

Die LED leuchtet, wenn sich der zugehörige Detektor/Switch im "abnormen" Zustand, d. h. dem Gegenteil des Normalzustands, befindet.

Die Bedeutung einer leuchtenden LED richtet sich nach den Einstellungen für den Normalzustand.

- **Normalzustand auf "Closed" (Geschlossen) festgelegt:**

LED	Sensorstatus
Leuchtet nicht	Closed (Geschlossen)
Leuchtet	Open (Offen)

- **Normalzustand auf "Open" (Offen) festgelegt:**

LED	Sensorstatus
Leuchtet nicht	Open (Offen)
Leuchtet	Closed (Geschlossen)

Anschließen von Differenzluftdrucksensoren

Wenn Sie Daten zum Differenzluftdruck benötigen, können Sie einen Differenzluftdrucksensor von Raritan an das EMX-Gerät anschließen.

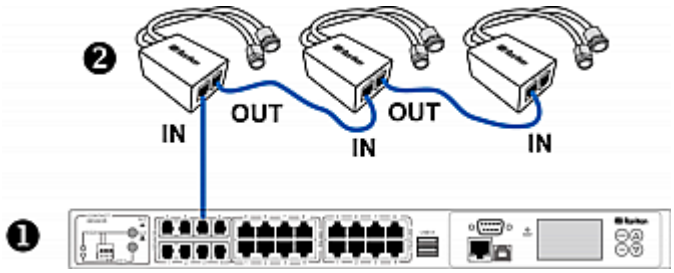
Mit diesem Sensor kann durch einen integrierten Temperatursensor auch die Temperatur um den Sensor herum ermittelt werden.

Mehrere Differenzluftdrucksensoren können hintereinandergeschaltet werden.

So schließen Sie einen Differenzluftdrucksensor an:

1. Schließen Sie ein Ende eines von Raritan mitgelieferten Telefonkabels an den SENSOR-Port des EMX-Geräts an.
2. Schließen Sie das andere Ende des Telefonkabels an den IN-Port des Differenzluftdrucksensors an.
3. So schließen Sie einen zusätzlichen Differenzluftdrucksensor von Raritan an:
   a. Schließen Sie ein Ende eines von Raritan mitgelieferten Telefonkabels an den OUT-Port des zuvor angeschlossenen Differenzluftdrucksensors an.
   b. Schließen Sie das andere Ende des Telefonkabels an den IN-Port des neu hinzugefügten Differenzluftdrucksensors an.
   c. Wiederholen Sie die Schritte a und b, um weitere Differenzialluftdrucksensoren hintereinanderzuschalten. Beachten Sie, dass jeder SENSOR-Port maximal 16 Umgebungssensoren unterstützt.

❶	EMX-Gerät
❷	Differenzluftdrucksensor von Raritan



Anschluss einer Logitech-Webcam (optional)

Die EMX-Einheit unterstützt Logitech® QuickCam® Pro 9000 Webcams, die daran angeschlossen sind, sodass Sie Video- oder Momentaufnahmen des Bereichs um die Webcam ansehen können. Das EMX 888-Gerät unterstützt bis zu zwei (2) Webcams, und das EMX 111-Gerät unterstützt eine (1) Webcam. Nachdem eine Webcam angeschlossen wurde, können Sie die Umgebungsbedingungen in der Nähe der EMX-Einheit von einem beliebigen Standort aus über die Webschnittstelle visuell überwachen.

Weitere Informationen zur QuickCam-Webcam finden Sie in der mitgelieferten Benutzerdokumentation.

So schließen Sie eine Webcam an:

1. Schließen Sie die Webcam an den USB-A-Port am EMX-Gerät an. Die EMX-Einheit erkennt die Webcam automatisch.
2. Positionieren Sie die Webcam ordnungsgemäß.

Von der Webcam erfasste statische Bilder oder Videos werden in der EMX-Webschnittstelle sofort angezeigt. Weitere Informationen zu dieser Funktion finden Sie unter ***Webcams*** (auf Seite 202). Informationen zum Konfigurieren der Webcam nach deren Anschluss finden Sie unter ***Konfigurieren von Webcams*** (auf Seite 203).

Hinweis: Um Webcams konfigurieren zu können, muss Ihrer Funktion die Berechtigung zum Ändern der Webcam-Konfiguration zugewiesen sein. Sie benötigen zudem die Berechtigung zum Anzeigen von Webcam-Bildern und Konfiguration, um Bilder in EMX anzeigen zu können.

Anschluss eines Schroff LHX-Wärmetauschers (optional)

Zur Remote-Überwachung und -Verwaltung der Schroff® LHX-20- oder LHX-40-Wärmetauscher über das EMX-Gerät müssen Sie eine Verbindung zwischen dem Wärmetauscher und dem EMX-Gerät herstellen.

Weitere Informationen zum LHX-Wärmetauscher finden Sie in der Benutzerdokumentation zum Produkt.

So schließen Sie einen LHX-Wärmetauscher an:

1. Schließen Sie ein Ende eines UTP-Standardkabels der Kategorie 5e/6 am RS-485-Port des Schroff LHX-Wärmetauschers an.
2. Schließen Sie das andere Ende des Kabels an einen der verfügbaren RS-485-Ports am EMX-Gerät an.

So schließen Sie einen LHX-Wärmetauscher über ein von Schroff bereitgestelltes serielles Kabel an den seriellen FEATURE-Port an:

1. Schließen Sie das DB9-Ende des Kabels an den RS232-Port des Schroff LHX-Wärmetauschers an.
2. Schließen Sie das andere Ende des Kabels an einen der verfügbaren seriellen FEATURE-Ports am EMX-Gerät an.

Informationen zum Überwachen und Verwalten des Wärmetauschers mithilfe des EMX-Geräts finden Sie unter ***Schroff LHX-Wärmetauscher*** (auf Seite 209).

Kapitel 3 Einführung

In diesem Kapitel

Unterstützte Webbrowser 41
Anschluss-Ports 41
LCD-Anzeigefeld 43
Reset-Taste 49
Anschluss des Kontaktschlusssensors 49
Netzschalter 49
Anmelden 50
Abmelden 51
Ändern des Kennworts 52
Einführung in die Webschnittstelle 53
Anzeigen des Dashboards 61

Unterstützte Webbrowser

Die folgenden Webbrowser können verwendet werden, um auf die Webschnittstelle von EMX zuzugreifen:

- Internet Explorer® 7 und 8
- Firefox® 3.x
- Safari® 5.1 (MacOS Lion)
- Konqueror
- Google® Chrome® 16.0

Folgende Smartphone-Browser werden unterstützt:

- Safari unter iOS 5.01
- Dolphin® 3.2.1

Anschluss-Ports

Die Anzahl der insgesamt verfügbaren Ports hängt vom Gerätemodell ab.

Die folgende Tabelle beschreibt die Funktion jedes Ports.

Port	Verwendung
USB-B	Zur Herstellung einer USB-Verbindung zwischen einem Computer und dem EMX-Gerät. Dieser Port kann zur Notfallwiederherstellung des EMX-Geräts verwendet werden. Wenden Sie sich an den technischen Kundendienst von Raritan, um Anweisungen zu erhalten.

Port	Verwendung
USB-A	Zum Anschließen eines USB-Geräts. Dies ist ein "Host"-Port, der entsprechend der USB-2.0-Spezifikationen mit Strom versorgt wird.
FEATURE	Anschluss an Assetsensoren über ein Kabel der Kategorie 5e/6. *Hinweis: Das EMX-Gerät versorgt die angeschlossenen Assetsensoren mit Strom, nachdem die Verbindung hergestellt wurde.*
CONSOLE/ MODEM	Zur Herstellung einer seriellen Verbindung zwischen einem Computer und dem EMX-Gerät: Dies ist ein Standard-DTE RS-232-Port. Sie können ein Nullmodemkabel mit zwei DB9-Steckern an beiden Enden verwenden, um das EMX-Gerät an den Computer anzuschließen.
SENSOR	Anschluss an die Umgebungssensoren von Raritan. Wenn mehrere Umgebungssensoren angeschlossen werden sollen, ist möglicherweise ein Raritan-Sensorhub erforderlich.
ETHERNET	Zur Verbindung des EMX-Geräts mit dem Netzwerk Ihres Unternehmens: Schließen Sie ein Ende eines Cat5e/6-UTP-Standardkabels an diesen Port an, und verbinden Sie das andere Ende mit dem Netzwerk. Diese Verbindung ist zur externen Verwaltung des EMX-Geräts oder den Zugriff auf das Gerät über die Webschnittstelle erforderlich. Neben dem Port befinden sich zwei kleine LEDs: ▪ Grünes Licht weist auf eine bestehende Verbindung und Aktivität hin. ▪ Gelbes Licht weist auf eine 10/100 BaseT-Kommunikation hin. Beim Hintereinanderschalten über USB ist die drahtgebundene Verbindung für die *Master*-EMX-Einheit unbedingt erforderlich. Weitere Informationen finden Sie im Abschnitt zum Hintereinanderschalten von PDUs über USB. *Hinweis: Der Anschluss an diesen Port ist nicht erforderlich, wenn das EMX-Gerät mit einem drahtlosen Netzwerk verbunden ist.*
RS-485	Anschluss an ein Elektrogerät mit RS-485-Schnittstelle. Derzeit unterstützt das EMX-Gerät nur Wärmetauscher vom Typ Schroff® LHX-20 und LHX-40.

LCD-Anzeigefeld

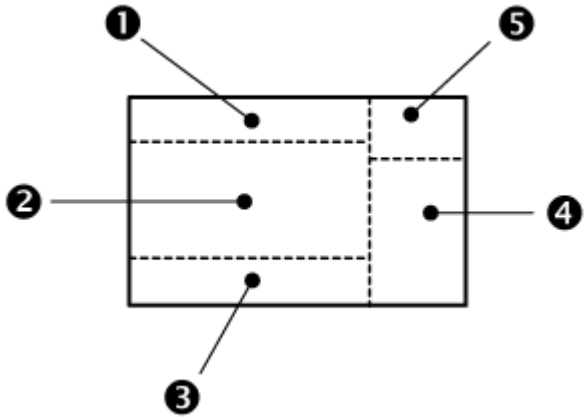
Das LCD-Anzeigefeld zeigt das Sensorergebnis oder den Sensorstatus, den Asset-Management-Status und die MAC-Adresse des Geräts an.

Es besteht aus den folgenden Komponenten:

- Einer LCD-Anzeige
- Bedienelementen

LCD-Anzeige

Verschiedene Arten von Informationen werden in verschiedenen Bereichen der LCD-Anzeige angezeigt. Die Bereiche sind im folgenden Schema dargestellt.



Bereich	Angezeigte Informationen
❶	Je nach Auswahl werden u. a. folgende Informationen angezeigt: • Der ausgewählte Umgebungssensor, einschließlich der ID-Nummer des Sensors. Das EMX-Gerät zeigt den ausgewählten Umgebungssensor auf zwei Arten an: ▪ Bei einem Sensor mit einer ID-Nummer unter 100 wird der Sensor als "SENSOR X" oder "SENSOR XX" angezeigt, wobei X und XX Ziffern sind. ▪ Bei einem Sensor mit einer ID-Nummer größer oder gleich 100 wird der Sensor als "1 SENSOR XX" angezeigt, wobei XX für die beiden letzten Ziffern der ID-Nummer steht. • Die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor angeschlossen ist.
❷	Je nach Auswahl werden u. a. folgende Informationen angezeigt: • Sensorergebnis aus Ziffern oder Sensorstatus aus Buchstaben • Nummer des SENSOR-Ports, an den der ausgewählte Sensor physisch angeschlossen ist • X-, Y- oder Z-Koordinaten des ausgewählten Umgebungssensors • Seriennummer des ausgewählten Umgebungssensors • Die Nummer der ausgewählten Rackeinheit für den ausgewählten Assetsensor *Hinweis: Bei einem Raritan-Assetsensor bezieht sich eine Rackeinheit auf einen Tag-Port.* • MAC-Adresse der EMX-Einheit

Bereich	Angezeigte Informationen
❸	Der Text "ALARM" kann angezeigt werden, um auf eines der folgenden Szenarien hinzuweisen: • Bei einem numerischen Umgebungssensor, z. B. einem Temperatursensor, bedeutet dies, dass das Sensormessergebnis den oberen oder unteren Schwellenwert erreicht bzw. über- oder unterschreitet, wenn diese Schwellenwerte aktiviert wurden. • Bei einem Einzel-Umgebungssensor (Ein/Aus-Sensor), z. B. einem Kontaktschlusssensor, bedeutet dies, dass der Sensor in den abnormalen Zustand wechselt. • Bei einem Assetsensor wird KEIN Asset-Tag an der ausgewählten Rackeinheit erkannt.
❹	Die Maßeinheit für den ausgewählten Umgebungssensor wird angezeigt. Die Maßeinheit variiert abhängig vom Sensortyp: • % wird bei einem Feuchtigkeitssensor angezeigt. • °C wird bei einem Temperatursensor angezeigt.
❺	Wird "ASSET" angezeigt, beziehen sich die angezeigten Informationen auf Assetsensoren und Asset-Tags.

Bedienelemente

Es gibt vier Bedienelemente.

- Die Tasten "Up" (Nach oben) und "Down" (Nach unten) zur Auswahl einer bestimmten ID oder Port-Nummer
- Taste MODE (Modus) zum Wechsel zwischen verschiedenen Arten von Zielinformationen, einschließlich Informationen zu Umgebungssensoren, Asset-Management-Informationen und MAC-Adresse
- Taste FUNC (FUNKTION) zum Wechsel zwischen verschiedenen Arten von Daten für einen ausgewählten Umgebungssensor

Das Anzeigefeld zeigt standardmäßig den ersten Umgebungssensor an, der auf der Seite "External Sensors" (Externe Sensoren) der Webschnittstelle aufgeführt ist, bis Sie einen anderen Umgebungssensor oder ein anderes Ziel auswählen.

Informationen zum Umgebungssensor

Die Informationen eines Umgebungssensors werden in der LCD-Anzeige als "SENSOR" eingeblendet. Zeigen Sie mithilfe der LCD-Anzeige Informationen zum ausgewählten Umgebungssensor an, einschließlich Sensormessergebnis oder -zustand, physische Port-Nummer des Sensors, X-, Y-, Z-Koordinaten und Seriennummer.

So zeigen Sie die Informationen eines Umgebungssensors an:

1. Drücken Sie die Taste "Up" (Nach oben) oder "Down" (Nach unten), bis die ID-Nummer des gewünschten Umgebungssensors oben in der LCD-Anzeige zu sehen ist. Siehe ***LCD-Anzeige*** (auf Seite 43). Beispielsweise steht "SENSOR 1" für Sensor 1 auf der Seite "External Sensors" (Externe Sensoren) der Webschnittstelle.
   - Drücken Sie die Taste △ (Nach oben), um die nächst höhere Option auszuwählen.
   - Drücken Sie die Taste ▽ (Nach unten), um die nächstniedrigere Option auszuwählen.
   - "1 SENSOR 24" bezieht sich auf Sensor 124.

   Hinweis: Halten Sie die Tasten "Up" (Nach oben) oder "Down" (Nach unten) mindestens zwei (2) Sekunden lang gedrückt, um schnell durch mehrere Einträge gleichzeitig zu wechseln.

2. Die LCD-Anzeige zeigt das Ergebnis oder den Status des ausgewählten Sensors in der Mitte der LCD-Anzeige.

   Beim Ergebnis eines numerischen Sensors wird die entsprechende Maßeinheit rechts neben dem Ergebnis eingeblendet.
   - % wird bei einem Feuchtigkeitssensor angezeigt.
   - °C wird bei einem Temperatursensor angezeigt.

   Bei einem Einzelsensor wird einer der folgenden Sensorzustände angezeigt:
   - on (ein): Der Sensor befindet sich im abnormen Zustand.
   - oFF (aus): Der Sensor befindet sich im Normalzustand.

   Hinweis: Numerische Sensoren verwenden numerische Werte, um die Umgebungs- oder internen Bedingungen anzugeben, während Einzelsensoren (Ein/Aus-Sensoren) alphabetische Zeichen zum Beschreiben des Status verwenden.

3. Wenn das EMX-Gerät über mehrere SENSOR-Ports verfügt, drücken Sie die Taste FUNC (Funktion), um die Nummer für den physischen Port des Umgebungssensors anzuzeigen. Die Port-Nummer wird als "P:X" angezeigt, wobei X die Port-Nummer ist. Der integrierte Kontaktschlusssensor wird als CC1 oder CC2 angezeigt.
4. Drücken Sie die Taste FUNC (Funktion), um die X-, Y- und Z-Koordinaten des Sensors anzuzeigen.
   - Die X-Koordinate wird als "x:XX" angezeigt, wobei XX für die ersten beiden Ziffern steht, die in der Webschnittstelle für die X-Koordinate eingegeben wurden.
   - Die Y-Koordinate wird als "y:XX" angezeigt, wobei XX für die ersten beiden Ziffern steht, die in der Webschnittstelle für die Y-Koordinate eingegeben wurden.
   - Die Z-Koordinate wird als "z:XX" angezeigt, wobei XX für die ersten beiden Ziffern steht, die in der Webschnittstelle für die Z-Koordinate eingegeben wurden.

   Wenn eine oder beide der ersten beiden Stellen einer bestimmten Koordinate Buchstaben sind, werden anstelle der Buchstaben ein bzw. zwei Unterstriche angezeigt.
5. Drücken Sie die Taste FUNC (Funktion) erneut, um die Seriennummer des Sensors anzuzeigen. Diese wird als "s:XX" angezeigt, wobei XX für zwei Stellen der Seriennummer steht. Die LCD-Anzeige wechselt von den ersten beiden bis zu den letzten beiden Stellen durch die Seriennummer.

   Wenn die Seriennummer beispielsweise AE17A00022 lautet, zeigt die LCD-Anzeige folgende Informationen nacheinander an:

   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

Wenn Sie nach Dutzenden von Sekunden keine Taste drücken, zeigt die LCD-Anzeige das Sensorergebnis oder den Status erneut an.

Asset-Management-Informationen

In der LCD-Anzeige können der Status des Assetsensors an jedem FEATURE-Port sowie der Asset-Tag-Status jeder Rackeinheit angezeigt werden. Bei einem Raritan-Assetsensor bezieht sich eine Rackeinheit auf einen Tag-Port.

So zeigen Sie die Asset-Management-Informationen an:

1. Drücken Sie die Taste MODE (Modus), bis oben rechts in der LCD-Anzeige "ASSET" zu sehen ist.
2. Drücken Sie die Taste "Up" (Nach oben) oder "Down" (Nach unten), bis die gewünschte FEATURE-Port-Nummer oben in der LCD-Anzeige zu sehen ist. Siehe ***LCD-Anzeige*** (auf Seite 43).

- Drücken Sie die Taste △ (Nach oben), um die nächst höhere Option auszuwählen.
- Drücken Sie die Taste ▽ (Nach unten), um die nächstniedrigere Option auszuwählen.

Wenn kein Assetsensor erkannt wird oder physisch an den ausgewählten FEATURE-Port angeschlossen ist, wird "nA" angezeigt.

Hinweis: Halten Sie die Tasten "Up" (Nach oben) oder "Down" (Nach unten) mindestens zwei (2) Sekunden lang gedrückt, um schnell durch mehrere Einträge gleichzeitig zu wechseln.

3. Drücken Sie die Taste FUNC (Funktion). Wenn links in der LCD-Anzeige ein blinkender Doppelpfeil ◇ angezeigt wird, wählen Sie mit der Taste "Up" (Nach oben) oder "Down" (Nach unten) die gewünschte Rackeinheit am momentan ausgewählten Assetsensor aus. Die Nummer der Rackeinheit wird in der Mitte der LCD-Anzeige eingeblendet.
   - Wird unter der Nummer der Rackeinheit "ALARM" angezeigt, wurde kein Asset-Tag erkannt oder es ist kein Asset-Tag physisch an die Rackeinheit angeschlossen.
   - Wird "ALARM" NICHT eingeblendet, wurde ein angeschlossenes Asset-Tag an der Rackeinheit erkannt.

MAC-Adresse

Die MAC-Adresse des EMX-Geräts kann über die LCD-Anzeige abgerufen werden. Mithilfe üblicher Netzwerktools können Sie die IP-Adresse des Geräts über die MAC-Adresse ermitteln. Wenden Sie sich an Ihren LAN-Administrator, wenn Sie Hilfe benötigen.

So zeigen Sie die MAC-Adresse an:

1. Drücken Sie die Taste MODE (Modus), bis der Buchstabe "M" links in der LCD-Anzeige eingeblendet wird.
2. Die MAC-Adresse wird als "M:XX" angezeigt, wobei XX für zwei Stellen der MAC-Adresse steht. Die LCD-Anzeige wechselt von den ersten beiden bis zu den letzten beiden Stellen durch die MAC-Adresse.

   Wenn die MAC-Adresse z. B. 00:0d:5d:03:5E:1A lautet, werden in der LCD-Anzeige nacheinander folgende Informationen eingeblendet:

   M:00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

Hinweis: Halten Sie die Tasten "Up" (Nach oben) oder "Down" (Nach unten) mindestens zwei (2) Sekunden lang gedrückt, um schnell durch mehrere Einträge gleichzeitig zu wechseln.

IP Address (IP-Adresse)

Die IP-Adresse ist auch in der LCD-Anzeige des EMX-Geräts verfügbar. Drücken Sie die Taste "Mode" (Modus), um zwischen Sensor-, Asset- und Gerätemodus zu wechseln. Im Gerätemodus wird links oben ein kleines "d" angezeigt. Die Adresse beginnt mit der IPv4-Adresse, was oben rechts in der Anzeige durch "i4" angegeben wird. Wechseln Sie mit der Taste "Function" (Funktion) zur MAC-Adresse. In diesem Fall wird rechts oben "M" angezeigt.

Reset-Taste

Die Reset-Taste befindet sich in einer kleinen Öffnung mit der Beschriftung RESET.

Über diese Taste kann die EMX-Einheit auf die werksseitigen Standardeinstellungen zurückgesetzt werden, sofern eine serielle Verbindung vorhanden ist. Siehe ***Wiederherstellen der werksseitigen Standardeinstellungen*** (auf Seite 103).

Ohne serielle Verbindung wird die Software des EMX-Geräts durch Drücken der Reset-Taste neu gestartet.

Anschluss des Kontaktschlusssensors

Modell EMX2-888 verfügt über zwei Channels für den Anschluss zweier Kontaktschlusssensoren anderer Hersteller.

Weitere Informationen finden Sie unter:

- ***Anschluss von Detektoren/Switches anderer Hersteller an das EMX-Gerät*** (auf Seite 36)
- ***LEDs des Kontaktschlusssensors*** (auf Seite 37)

Netzschalter

Das EMX-Gerät lässt sich mit dem Netzschalter ein- und ausschalten.

Um das EMX-Gerät aus- und wieder einzuschalten, drücken Sie den Netzschalter, um das Gerät auszuschalten. **Warten Sie mindestens 10 Sekunden**, und drücken Sie dann den Netzschalter noch einmal, um es einzuschalten. Beachten Sie, dass das Gerät mindestens 10 Sekunden ausgeschaltet sein muss, weil es sonst nicht ordnungsgemäß bootet.

Anmelden

Zur Anmeldung bei der Webschnittstelle müssen Sie einen Benutzernamen und ein Kennwort eingeben. Verwenden Sie für die ersten Anmeldung bei EMX den Standardbenutzernamen (admin) und das Standardkennwort (raritan). Aus Sicherheitsgründen werden Sie danach zur Änderung des Kennworts aufgefordert.

Ausnahme: Wenn Sie das Kennwort für das Administratorkonto bereits während der Erstkonfiguration des Netzwerks geändert haben, verwenden Sie stattdessen das neue Kennwort, um sich bei der Webschnittstelle anzumelden. Die EMX-Einheit fordert Sie in diesem Fall NICHT zum Ändern des Kennworts auf.

Nach erfolgreicher Anmeldung können Sie Benutzerprofile für die übrigen Benutzer erstellen. Mit diesen Profilen werden die Anmeldenamen und -kennwörter dieser Benutzer definiert. Siehe ***Erstellen von Benutzerprofilen*** (auf Seite 62).

Die Webschnittstelle ermöglicht die gleichzeitige Anwendung von maximal 16 Benutzern.

Für eine ordnungsgemäße Funktion muss im Webbrowser JavaScript aktiviert sein.

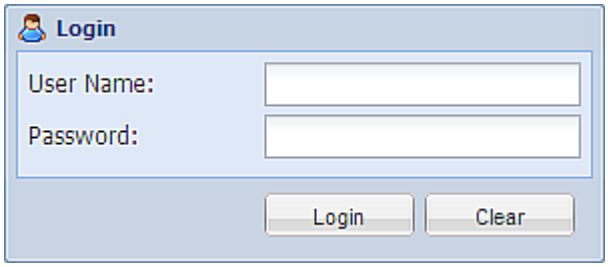
So melden Sie sich bei der Webschnittstelle an:

1. Öffnen Sie einen Browser, wie Microsoft Internet Explorer oder Mozilla Firefox, und geben Sie den folgenden URL ein:

   http(s)://<IP-Adresse>.

   Dabei steht *<IP-Adresse>* für die IP-Adresse des EMX-Geräts.

2. Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf "OK" oder auf "Yes" (Ja), um sie zu akzeptieren. Die Anmeldeseite wird angezeigt.



3. Geben Sie im Feld "Username" (Benutzername) Ihren Benutzernamen und im Feld "Password" (Kennwort) Ihr Kennwort ein.

Hinweis: Bei beiden Feldern ist die Groß-/Kleinschreibung zu beachten. Wenn Sie sie falsch eingegeben haben, klicken Sie auf "Clear" (Löschen), um die Eingaben zu löschen oder angezeigte Fehlermeldungen zu schließen.

4. Klicken Sie auf "Login" (Anmelden), oder drücken Sie die Eingabetaste. Die Seite EMX wird geöffnet.

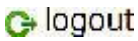
Hinweis: Die auf der Seite EMX angezeigten Elemente können sich je nach Hardware-Konfiguration von dieser Abbildung unterscheiden.

Abmelden

Nachdem Sie die Aufgaben für die EMX-Einheit abgeschlossen haben, müssen Sie sich abmelden, damit keine anderen Personen auf die Webschnittstelle zugreifen können.

So melden Sie sich bei der Webschnittstelle ab:

1. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie in der oberen rechten Ecke der Webschnittstelle auf "logout" (Abmelden).

   - Schließen Sie den Webbrowser, indem Sie auf die Schließen-Schaltfläche ( ) in der oberen rechten Ecke des Browsers klicken.
   - Schließen Sie den Webbrowser, indem Sie "File" > "Close" (Datei > Schließen) oder "File" > "Exit" (Datei > Beenden) auswählen. Der Name des Befehls hängt von der verwendeten Browserversion ab.
   - Wählen Sie den Befehl "Refresh" (Aktualisieren), oder klicken Sie auf die Schaltfläche "Refresh" (Aktualisieren) im Webbrowser.
2. Entweder wird die Anmeldeseite geöffnet, oder der Browser wird geschlossen. Dies hängt von der Auswahl im vorherigen Schritt ab.

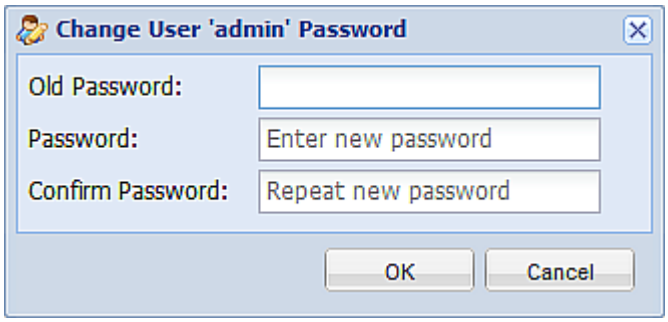
Ändern des Kennworts

Normale Benutzer können ihre eigenen Kennwörter ändern, wenn sie die Berechtigung "Change Own Password" (Eigenes Kennwort ändern) haben. Siehe ***Einrichten von Benutzerfunktionen*** (auf Seite 70).

Als Administrator (admin) werden Sie von der EMX-Webschnittstelle automatisch aufgefordert, das Kennwort zu ändern, wenn Sie sich erstmals bei der EMX-Einheit anmelden. Wenn Sie über Administratorberechtigung verfügen, können Sie die Kennwörter anderer Benutzer ändern. Siehe ***Ändern von Benutzerprofilen*** (auf Seite 67).

So ändern Sie Ihr Kennwort:

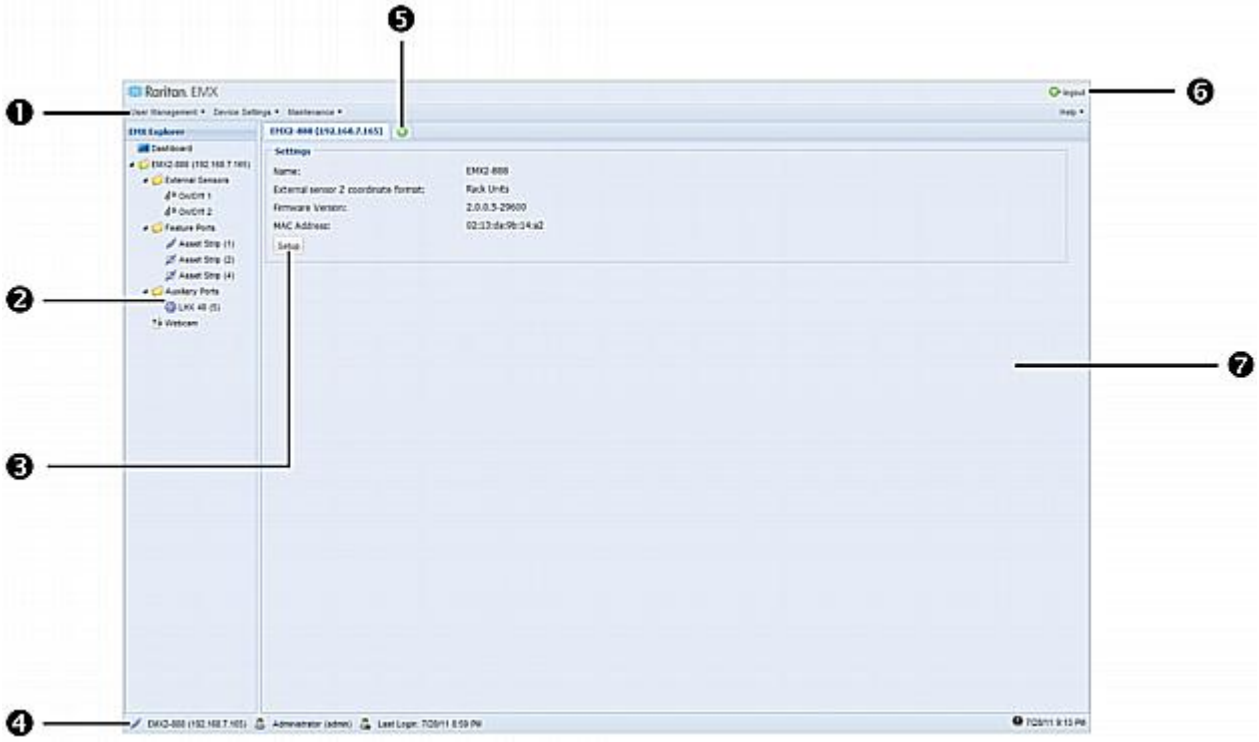
1. Wählen Sie "User Management" > "Change Password" (Benutzerverwaltung > Kennwort ändern) aus. Das Dialogfeld "Change User Password" (Benutzerkennwort ändern) wird angezeigt.



2. Geben Sie im Feld "Old Password" (Altes Kennwort) Ihr derzeitiges Kennwort ein.
3. Geben Sie Ihr neues Kennwort in die Felder "Password" (Kennwort) und "Confirm Password" (Kennwort bestätigen) ein. Das Kennwort kann 4 bis 64 Zeichen enthalten. Die Groß-/Kleinschreibung muss beachtet werden.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Einführung in die Webschnittstelle

Die Webschnittstelle enthält auf jeder Seite zwei Fensterbereiche, eine Menüleiste, eine Statusleiste, ein Symbol "Add Page" (Seite hinzufügen) und eine Schaltfläche für das Abmelden.



Nummer	Elemente der Webschnittstelle
❶	Menüs
❷	Fenster "EMX Explorer"
❸	Schaltfläche "Setup"* (Einrichten)
❹	Statusleiste
❺	Symbol "Add Page" (Seite hinzufügen)
❻	Schaltfläche "Logout" (Abmelden)
❼	Datenfenster

* Die Schaltfläche "Setup" (Einrichten) steht auf einigen Seiten, wie z. B. die Seite *Dashboard* nicht zur Verfügung.

Detailliertere Informationen zu den Elementen der Webschnittstelle finden Sie in den folgenden Abschnitten.

Menüs

Für das Verwalten verschiedener Aufgaben oder zum Anzeigen von Informationen stehen vier Menüs zur Verfügung.

- **User Management** (Benutzerverwaltung) enthält Menüoptionen zum Verwalten von Benutzerprofilen, Berechtigungen (Benutzerfunktionen) und Kennwörtern.
- **Device Settings** (Geräteeinstellungen) enthält Einstellungen für das Gerät, wie z. B. Gerätename, Netzwerkeinstellungen, Sicherheitseinstellungen und Systemzeit.
- **Maintenance** (Wartung) enthält Tools zum Warten der EMX-Einheit, wie z. B. Ereignisprotokoll, Hardwareinformationen, Firmware-Aktualisierung usw.
- **Help** (Hilfe) zeigt Informationen zur Firmware sowie zu allen OpenSource-Paketen an, die in das EMX-Gerät eingebettet sind. Außerdem können Sie in diesem Menü das Benutzerhandbuch aufrufen.

Schaltfläche "Setup" (Einrichten)

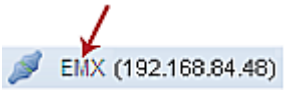
Die Schaltfläche "Setup" (Einrichten) steht für die meisten Elemente der Verzeichnisstruktur zur Verfügung. Mit der Schaltfläche öffnen Sie ein Dialogfeld, in dem Sie die Einstellungen für das ausgewählte Element der Verzeichnisstruktur ändern können.

Statusleiste

Die Statusleiste zeigt von links nach rechts fünf verschiedene Informationen an.

- **Gerätename:**

  Dies ist der Name, der dem EMX-Gerät zugewiesen ist. Standardmäßig wird der Name "EMX" verwendet. Siehe ***Benennen des EMX-Geräts*** (auf Seite 74).



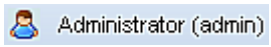
- **IP-Adresse:**

  Die in Klammern enthaltenen Nummern stellen die IP-Adresse dar, die dem EMX-Gerät zugewiesen ist. Siehe Erstkonfiguration des Netzwerks oder ***Ändern der Netzwerkeinstellungen*** (auf Seite 84).

Tipp: Wenn der Gerätename und die IP-Adresse in der Statusleiste angezeigt werden, ist die Verbindung zum EMX-Gerät hergestellt.
Wenn die Verbindung verloren geht, wird " disconnected *" angezeigt.*

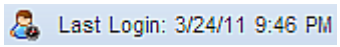
- **Anmeldename:**

  Dies ist der Benutzername, mit dem Sie sich bei der Webschnittstelle anmelden.

- **Last login time (Letzte Anmeldung):**

  Hier werden Datum und Uhrzeit der letzten Anmeldung des Benutzernamens bei diesem EMX-Gerät angezeigt.

  Wenn Sie den Mauszeiger über den Zeitpunkt der letzten Anmeldung ziehen, werden detaillierte Informationen über die letzte Anmeldung angezeigt, einschließlich Client und IP-Adresse des Zugriffs.

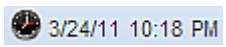
  Bei der Anmeldung über eine serielle Verbindung wird statt einer IP-Adresse <local> angezeigt.

  Es gibt verschiedene Typen von Zugriff-Clients:

  - Web-GUI: Bezieht sich auf die Webschnittstelle von EMX.
  - CLI: Bezieht sich auf die Befehlszeilenschnittstelle (CLI).
    Die Informationen in Klammern hinter "CLI" zeigen an, wie dieser Benutzer mit der Befehlszeilenschnittstelle verbunden ist.
    - *Serial (Seriell)*: Gibt die lokale Verbindung an (seriell oder USB).
    - *SSH*: Gibt die SSH-Verbindung an.
    - *Telnet*: Gibt die Telnet-Verbindung an.

- **Systemdatum und Uhrzeit:**

  Aktuelles Datum, Jahr und Uhrzeit werden rechts in der Leiste angezeigt. Wenn Sie den Mauszeiger auf das Systemdatum und die Uhrzeit ziehen, werden auch Informationen zur Zeitzone angezeigt.

Manchmal wird rechts in der Leiste eine Fahne () angezeigt, wenn ein Kommunikationsfehler zwischen dem EMX-Gerät und der grafischen Benutzeroberfläche aufgetreten ist. Klicken Sie in diesem Fall auf das Symbol, um das Kommunikationsprotokoll anzuzeigen. Siehe ***Anzeigen des Kommunikationsprotokolls*** (auf Seite 168).

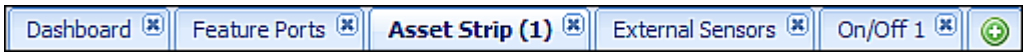
Symbol "Add Page" (Seite hinzufügen)

Mit dem Symbol "Add Page" (Seite hinzufügen) , das sich oben im Datenfenster befindet, können Sie Datenfenster mehrerer Elemente der Verzeichnisstruktur öffnen, ohne eine geöffnete Seite zu überschreiben.

So öffnen Sie neue Datenseiten:

1. Klicken Sie auf das Symbol "Add Page" (Seite hinzufügen) . Eine neue Registerkarte wird mit einer leeren Datenseite angezeigt.
2. Klicken Sie auf ein Element der Verzeichnisstruktur, dessen Datenseite Sie öffnen möchten. Die Daten des ausgewählten Elements der Verzeichnisstruktur werden dann auf der leeren Seite angezeigt.
3. Um weitere Datenseiten zu öffnen, wiederholen Sie die Schritte 1 bis 2. Alle Registerkarten, die die geöffneten Seiten enthalten, werden oben auf der Seite angezeigt.

   Die folgende Abbildung enthält ein Beispiel von mehreren Registerkarten.



4. Wenn mehrere Seiten geöffnet sind, können Sie Folgendes ausführen:
   - Um zu einer der geöffneten Datenseiten zu wechseln, klicken Sie auf das entsprechende Register.

     Wenn nicht alle Registerkarten angezeigt werden können, werden am linken und rechten Rand des Fensterbereichs zwei Pfeile (und) angezeigt. Klicken Sie auf einen Pfeil, um durch alle Registerkarten zu navigieren.
   - Um eine Datenseite zu schließen, klicken Sie auf der entsprechenden Registerkarte auf die Schließen-Schaltfläche ( ).

Datenfenster

Der rechte Fensterbereich zeigt die Datenseite des ausgewählten Elements der Verzeichnisstruktur an. Auf der Datenseite werden der aktuelle Status, die Einstellungen sowie die Schaltfläche "Setup" (Einrichten) für das Element angezeigt.

Alle Register über dem Fensterbereich entsprechen den geöffneten Datenseiten. Das hervorgehobene Register gibt die aktuelle Auswahl an.

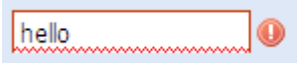
Sie können die Breite des Fensters ändern, um den Bereich zu vergrößern oder zu verkleinern.

So passen Sie die Breite des Fensterbereichs an:

1. Ziehen Sie den Mauszeiger auf den linken Rand des rechten Fensterbereichs.
2. Wenn der Mauszeiger als Doppelpfeil angezeigt wird, ziehen Sie den Rahmen horizontal, um das Fenster zu vergrößern oder zu verkleinern.

Warnsymbol

Wenn der in einem bestimmten Feld eingegebene Wert ungültig ist, wird rechts ein rotes Alarmsymbol angezeigt und das entsprechende Feld wird durch einen roten Rahmen gekennzeichnet (siehe Abbildung).



Ziehen Sie in diesem Fall den Mauszeiger über das Warnsymbol, um die Ursache anzuzeigen, und ändern Sie den eingegebenen Wert entsprechend ab.

Gelb oder Rot hervorgehobene Ergebnisse

Wenn eine Messung eines numerischen Sensors einen oberen oder unteren Schwellenwert überschreitet, wird der Hintergrund der gesamten Zeile gelb oder rot angezeigt, um die Benutzer zu warnen.

Bei einem Einzelsensor (Ein/Aus-Sensor) ändert sich die Hintergrundfarbe der Zeile, wenn der Sensor in den abnormalen Zustand wechselt.

Hinweis: Numerische Sensoren verwenden numerische Werte, um die Umgebungs- oder internen Bedingungen anzugeben, während Einzelsensoren (Ein/Aus-Sensoren) alphabetische Zeichen zum Beschreiben des Status verwenden.

In der folgenden Tabelle werden die Farben erläutert:

Farbe	Status
Weiß	Der Hintergrund ist in einem der folgenden Szenarien weiß: • Für einen numerischen Sensor wurden keine Schwellenwerte aktiviert. • Wenn Schwellenwerte für einen numerischen Sensor aktiviert wurden, liegt das Sensormessergebnis zwischen dem unteren und dem oberen Warnschwellenwert. • Für einen Einzelsensor (Ein/Aus-Sensor) ist der Sensorzustand normal. • Das Sensormessergebnis oder der Sensorzustand ist "nicht verfügbar".
Gelb	Das Ergebnis fällt unter den unteren Warnschwellenwert oder steigt über den oberen Warnschwellenwert.
Red (Rot)	Die Bedeutung für Rot hängt vom Sensortyp ab: • Für einen numerischen Sensor bedeutet diese Farbe, dass das Ergebnis unter den unteren kritischen Schwellenwert gefallen oder über den oberen kritischen Schwellenwert gestiegen ist. • Für einen Einzelsensor (Ein/Aus-Sensor) bedeutet diese Farbe, dass sich der Sensor im Zustand "alarmed" (Alarm) befindet. • Bei einem Schroff® LHX-Wärmetauscher (sofern verfügbar) bedeutet diese Farbe, dass mindestens ein auf diesem Wärmetauscher implementierter Sensor ausgefallen ist. Siehe ***Schroff LHX-Wärmetauscher*** (auf Seite 209).

Die genaue Bedeutung des Alarms finden Sie in den Informationen in der Spalte "State" (Zustand) oder "Status":

- below lower critical (unter unterem kritischen Schwellenwert): Das Ergebnis des numerischen Sensors fällt unter den unteren kritischen Schwellenwert.
- below lower warning (unter unterem Warnschwellenwert): Das Ergebnis des numerischen Sensors fällt unter den unteren Warnschwellenwert.
- above upper critical (über oberem kritischen Schwellenwert): Das Ergebnis des numerischen Sensors erreicht oder übersteigt den oberen kritischen Schwellenwert.
- above upper warning (über oberem Warnschwellenwert): Das Ergebnis des numerischen Sensors erreicht oder übersteigt den oberen Warnschwellenwert.
- alarmed (Alarmzustand): Der Einzelsensor befindet sich NICHT im Normalzustand.

Weitere Informationen über die Schwellenwerte finden Sie unter ***Konfigurieren von Umgebungssensoren*** (auf Seite 177).

Durch den Browser definiertes Kontextmenü

Ein Kontextmenü, das im Webbrowser integriert ist, wird angezeigt, wenn Sie in der EMX-Webschnittstelle mit der rechten Maustaste auf eine beliebige Stelle klicken.

Die Kontextmenüfunktionen werden vom Browser definiert. Beispielsweise ist die Funktionsweise des Befehls "Zurück" im Kontextmenü des Internet Explorer® (IE) identisch mit der Zurück-Schaltfläche im IE-Browser. Beide Möglichkeiten können verwendet werden, um zur vorherigen Seite zurückzukehren.

Weitere Informationen zu jedem Befehl oder jeder Option im Kontextmenü finden Sie in der Online-Hilfe oder in der Dokumentation, die mit dem Webbrowser ausgeliefert wird.

Die nachfolgende Abbildung zeigt das Kontextmenü des IE-Browsers. Verfügbare Menübefehle oder -optionen in Ihrer Webbrowser-Version können sich von der Abbildung unterscheiden.

Anzeigen des Dashboards

Wenn Sie sich bei der Webschnittstelle anmelden, wird standardmäßig die Seite "Dashboard" angezeigt. Diese Seite bietet eine Übersicht über den Status des EMX-Geräts.

Die Seite ist entsprechend den angeschlossenen Geräten in mehrere Bereiche unterteilt, z. B. Assetsensoren und Umgebungssensoren. Durch einen Doppelklick auf ein Element auf der Seite "Dashboard" wird die Datenseite geöffnet, die zum ausgewählten Element gehört.

Hinweis: Eine farbig dargestellte Zeile mit einem Sensorergebnis weist darauf hin, dass das Sensorergebnis bereits einen Schwellenwert über- oder unterschreitet oder dass mindestens ein integrierter LHX-Sensor am Wärmetauscher ausgefallen ist. Siehe **Gelb oder Rot hervorgehobene Ergebnisse (EMX)** *(siehe "***Gelb oder Rot hervorgehobene Ergebnisse***" auf Seite 58).*

Nachdem Sie in der hierarchischen Verzeichnisstruktur auf ein beliebiges Symbol geklickt habe, wird die Seite "Dashboard" übersprungen. Um zur Seite "Dashboard" zurückzukehren, klicken Sie auf das Symbol "Dashboard".

Wenn die Seite "Dashboard" geöffnet wird, können Sie bestimmte Daten anzeigen oder ausblenden.

So blenden Sie einen Bereich aus:

1. Suchen Sie den Bereich, den Sie ausblenden möchten.
2. Klicken Sie vor dem Namen des Bereichs auf den Pfeil nach oben . Die Daten für diesen Bereich werden ausgeblendet.

So zeigen Sie einen ausgeblendeten Bereich an:

1. Suchen Sie den Bereich, den Sie anzeigen möchten.
2. Klicken Sie vor dem Namen des Bereichs auf den Pfeil nach unten . Die Daten für diesen Bereich werden angezeigt.

Kapitel 4 Verwaltung von Benutzern und Benutzerfunktionen

In diesem Kapitel

Übersicht.....62
Verwalten von Benutzern 62
Verwalten von Benutzerfunktionen.....70

Übersicht

Auf der EMX-Einheit ist ein Benutzerprofil vordefiniert: **admin**, das für die erste Anmeldung und Konfiguration verwendet wird. Dieses Profil verfügt über uneingeschränkte Systemberechtigungen und sollte für den Systemadministrator reserviert werden. Es kann weder gelöscht werden, noch können die Berechtigungen, mit Ausnahme der SNMP-v3-Berechtigung, geändert werden.

Alle Benutzer müssen ein Benutzerprofil aufweisen, das einen Namen und ein Kennwort für die Anmeldung und optional weitere Informationen zum Benutzer enthält. Jedes Benutzerprofil muss mindestens eine Benutzerfunktion aufweisen, um die Systemberechtigungen des Benutzers festzulegen. Siehe ***Einrichten von Benutzerfunktionen*** (auf Seite 70). Zum Verwalten von Einstellungen müssen Sie sich mit den entsprechenden Berechtigungen beim Benutzerkonto anmelden.

Standardmäßig können sich mehrere Benutzer gleichzeitig mit demselben Anmeldenamen anmelden.

Verwalten von Benutzern

Erstellen von Benutzerprofilen

Beim Erstellen neuer Benutzer wird der EMX-Einheit eine neue Anmeldung hinzugefügt.

So erstellen Sie ein Benutzerprofil:

1. Wählen Sie "User Management" > "Users" (Benutzerverwaltung > Benutzer) aus. Das Dialogfeld "Manage Users" (Benutzer verwalten) wird angezeigt.
2. Klicken Sie auf "New" (Neu). Das Dialogfeld "Create New User" (Neuen Benutzer erstellen) wird angezeigt.

3. Geben Sie die Informationen zum Benutzer in die entsprechenden Felder ein. Die Felder "User Name" (Benutzername), "Password" (Kennwort) und "Confirm Password" (Kennwort bestätigen) sind erforderlich.

Feld	Eingabe
User Name (Benutzername)	Name, den der Benutzer zur Anmeldung bei der EMX-Einheit eingibt. ▪ Der Name kann 4 bis 32 Zeichen enthalten. ▪ Die Groß-/Kleinschreibung muss beachtet werden. ▪ Leerstellen sind NICHT zulässig.
Full Name (Vollständiger Name)	Vor- und Nachname des Benutzers
Password (Kennwort) Confirm Password (Kennwort bestätigen)	Kennwort, das der Benutzer zur Anmeldung eingibt. Geben Sie das Kennwort zunächst im Feld "Password" (Kennwort) und anschließend im Feld "Confirm Password" (Kennwort bestätigen) ein. ▪ Das Kennwort kann 4 bis 32 Zeichen enthalten. ▪ Die Groß-/Kleinschreibung muss beachtet werden. ▪ Leerstellen sind zulässig.
Telephone Number (Telefonnummer)	Telefonnummer, unter der der Benutzer zu erreichen ist.
email Address (E-Mail-Adresse)	E-Mail-Adresse des Benutzers ▪ Die E-Mail-Adresse kann 4 bis 32 Zeichen enthalten. ▪ Die Groß-/Kleinschreibung muss beachtet werden.

4. Wählen Sie das Kontrollkästchen "Enabled" (Aktiviert) aus. Andernfalls kann sich der Benutzer NICHT bei EMX anmelden.
5. Aktivieren Sie das Kontrollkästchen "Force password change on next login" (Kennwortänderung bei nächster Anmeldung erzwingen), wenn der Benutzer das Kennwort ändern soll, wenn er sich erstmals anmeldet, nachdem das Kontrollkästchen aktiviert wurde.
6. Klicken Sie auf die Registerkarte "SNMPv3", um die SNMPv3-Zugriffsberechtigung zu aktivieren. Standardmäßig ist die Berechtigung deaktiviert.

a. Um den Zugriff auf SNMPv3 durch diesen Benutzer zu erlauben, aktivieren Sie das Kontrollkästchen "Enable SNMPv3 access" (SNMPv3-Zugriff aktivieren). Andernfalls lassen Sie das Kontrollkästchen deaktiviert.

Hinweis: Das SNMPv3-Protokoll muss für den SNMPv3-Zugriff aktiviert sein. Siehe **Konfigurieren der SNMP-Einstellungen** *(auf Seite 90).*

b. Stellen Sie die SNMPv3-Parameter ein, wenn Sie die SNMPv3-Zugriffsberechtigung aktiviert haben.

Feld	Beschreibung
Security Level (Sicherheitsebene)	Klicken Sie auf die Dropdown-Liste, um die bevorzugte Sicherheitsebene aus der Liste auszuwählen. ▪ NoAuthNoPriv: Keine Authentifizierung und kein exklusiver Zugriff. ▪ AuthNoPriv: Authentifizierung und kein exklusiver Zugriff. ▪ AuthPriv: Authentifizierung und exklusiver Zugriff. Dies ist die Standardeinstellung.
Use Password as Authentication Pass Phrase (Kennwort als Passphrase für Authentifizierung verwenden)	*Dieses Kontrollkästchen ist nur konfigurierbar, wenn "AuthNoPriv" oder "AuthPriv" ausgewählt ist.* Wenn das Kontrollkästchen aktiviert ist, ist die Passphrase für die Authentifizierung mit dem Benutzerkennwort identisch. Um eine andere Passphrase für die Authentifizierung anzugeben, deaktivieren Sie das Kontrollkästchen.
Authentication Pass Phrase (Passphrase für Authentifizierung)	Geben Sie die Passphrase für die Authentifizierung in dieses Feld ein, wenn das Kontrollkästchen "Use Password as Authentication Pass Phrase" (Kennwort als Passphrase für Authentifizierung verwenden) deaktiviert ist. Die Passphrase muss aus 8 bis 32 druckbaren ASCII-Zeichen bestehen.
Confirm Authentication Pass Phrase (Passphrase für Authentifizierung bestätigen)	Geben Sie zum Bestätigen dieselbe Passphrase für die Authentifizierung erneut ein.
Use Authentication	*Dieses Kontrollkästchen ist nur konfigurierbar,*

Feld	Beschreibung
Pass Phrase as Privacy Pass Phrase (Passphrase für Authentifizierung als Passphrase für exklusiven Zugriff verwenden)	*wenn "AuthPriv" ausgewählt ist.* Wenn das Kontrollkästchen aktiviert ist, ist die Passphrase für den exklusiven Zugriff mit der Passphrase für Authentifizierung identisch. Um eine andere Passphrase für den exklusiven Zugriff anzugeben, deaktivieren Sie das Kontrollkästchen.
Privacy Pass Phrase (Passphrase für exklusiven Zugriff)	Geben Sie die Passphrase für den exklusiven Zugriff in dieses Feld ein, wenn das Kontrollkästchen "Use Authentication Pass Phrase as Privacy Pass Phrase" (Passphrase für Authentifizierung als Passphrase für exklusiven Zugriff verwenden) deaktiviert ist. Die Passphrase muss aus 8 bis 32 druckbaren ASCII-Zeichen bestehen.
Confirm Privacy Pass Phrase (*Passphrase für exklusiven Zugriff bestätigen)	Geben Sie zum Bestätigen dieselbe Passphrase für den exklusiven Zugriff erneut ein.
Authentication Protocol (Authentifizierungsprotokoll)	Klicken Sie auf die Dropdown-Liste, um das gewünschte Authentifizierungsprotokoll aus der Liste auszuwählen. Es stehen zwei Protokolle zur Verfügung: ▪ MD5 ▪ SHA-1 (Standard)
Privacy Protocol (Protokoll für exklusiven Zugriff)	Klicken Sie auf die Dropdown-Liste, um das gewünschte Protokoll für den exklusiven Zugriff aus der Liste auszuwählen. Es stehen zwei Protokolle zur Verfügung: ▪ DES (Standard) ▪ AES-128

7. Klicken Sie auf die Registerkarte "SSH", um den öffentlichen Schlüssel einzugeben, wenn die Authentifizierung mit öffentlichem Schlüssel für den SSH-Dienst aktiviert ist. Siehe ***Ändern der SSH-Einstellungen*** (auf Seite 90).
   a. Öffnen Sie den öffentlichen SSH-Schlüssel mit einem Texteditor.
   b. Kopieren Sie den gesamten Inhalt im Texteditor in das Feld "Public Key" (Öffentlicher Schlüssel) auf der Registerkarte "SSH".

8. Klicken Sie auf die Registerkarte "Roles" (Benutzerfunktionen), um die Berechtigungen des Benutzers festzulegen.
9. Wählen Sie eine oder mehrere Benutzerfunktionen, indem Sie die entsprechenden Kontrollkästchen aktivieren.
   - Die Benutzerfunktion "Admin" verfügt über uneingeschränkte Berechtigungen.
   - Die Benutzerfunktion "Operator" verfügt über eingeschränkte Berechtigungen für häufig verwendete Funktionen. Informationen zum Umfang der Berechtigungen finden Sie unter ***Einrichten von Benutzerfunktionen*** (auf Seite 70). Diese Benutzerfunktion ist standardmäßig ausgewählt.
   - Wenn keine Benutzerfunktionen Ihre Anforderungen erfüllen, können Sie Folgendes ausführen:
     - *Ändern Sie die Berechtigungen einer vorhandenen Benutzerfunktion:* Um die Berechtigungen einer beliebigen Benutzerfunktion zu ändern, doppelklicken Sie auf die Benutzerfunktion oder markieren sie diese und klicken Sie anschließend auf "Edit Role" (Benutzerfunktion bearbeiten). Siehe ***Ändern von Benutzerfunktionen*** (auf Seite 71).
     - *Erstellen Sie eine neue Benutzerfunktion, indem Sie auf die Schaltfläche "Manage Roles" (Benutzerfunktionen verwalten) klicken:* Siehe ***Erstellen einer Benutzerfunktion*** (auf Seite 70).

   Hinweis: Wenn mehrere Benutzerfunktionen ausgewählt sind, verfügt der Benutzer über die Berechtigungen aller Benutzerfunktionen.
10. Um die für diesen Benutzer in der Webschnittstelle angezeigten Maßeinheiten zu ändern, klicken Sie auf die Registerkarte "Preferences" (Einstellungen) und führen Sie eine der folgenden Aktionen durch:
    - Wählen Sie im Feld "Temperature Unit" (Temperatureinheit) °C (Celsius) oder °F (Fahrenheit) als Maßeinheit für Temperaturen.
    - Wählen Sie im Feld "Length" (Länge) "Meter" oder "Feet" (Fuß) als Maßeinheit für die Länge oder Höhe.
    - Wählen Sie im Feld "Pressure" (Druck) "Pascal" oder "psi" als Maßeinheit für Druck.

    Ein Pascal entspricht 1 Newton pro Quadratmeter. Psi steht für Pounds per Square Inch (Pfund pro Quadratzoll).

    Hinweis: Die Änderung der Messeinheit gilt nur für die Webschnittstelle und die Befehlszeilenschnittstelle.
11. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern von Benutzerprofilen

Sie können die Informationen eines beliebigen Benutzerprofils ändern, jedoch nicht den Benutzernamen.

So ändern Sie ein Benutzerprofil:

1. Wählen Sie "User Management" > "Users" (Benutzerverwaltung > Benutzer) aus. Das Dialogfeld "Manage Users" (Benutzer verwalten) wird angezeigt.
2. Wählen Sie den Benutzer aus, indem Sie auf ihn klicken.
3. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf den Benutzer. Das Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) wird angezeigt, wobei XXX den Benutzernamen darstellt.
4. Nehmen Sie an den angezeigten Informationen die erforderlichen Änderungen vor.

   Um das Kennwort zu ändern, geben Sie in den Feldern "Password" (Kennwort) und "Confirm Password" (Kennwort bestätigen) ein neues Kennwort ein. Wenn Sie diese Felder leer lassen, wird das Kennwort nicht geändert.
5. Um die Zugriffsberechtigungen von SNMPv3 zu ändern, klicken Sie auf die Registerkarte "SNMPv3" und nehmen die erforderlichen Änderungen vor. Weitere Einzelheiten finden Sie unter ***Erstellen von Benutzerprofilen*** (auf Seite 62) in Schritt 6.
6. Um die Berechtigungen zu ändern, klicken Sie auf die Registerkarte "Roles" (Benutzerfunktionen) und führen einen der folgenden Schritte aus:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen einer beliebigen Benutzerfunktion.
   - Um die Berechtigungen einer beliebigen Benutzerfunktion zu ändern, doppelklicken Sie auf die Benutzerfunktion oder markieren sie diese und klicken Sie anschließend auf "Edit Role" (Benutzerfunktion bearbeiten). Siehe ***Ändern von Benutzerfunktionen*** (auf Seite 71).
7. Um die Maßeinheit für Temperatur, Länge oder Druck zu ändern, klicken Sie auf die Registerkarte "Preferences" (Einstellungen) und wählen Sie eine andere Option aus der Dropdown-Liste aus.

   Hinweis: Die Änderung der Messeinheit gilt nur für die Webschnittstelle und die Befehlszeilenschnittstelle.
8. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen von Benutzerprofilen

Löschen Sie gegebenenfalls veraltete oder redundante Benutzerprofile.

So löschen Sie Benutzerprofile:

1. Wählen Sie "User Management" > "Users" (Benutzerverwaltung > Benutzer) aus. Das Dialogfeld "Manage Users" (Benutzer verwalten) wird angezeigt.
2. Klicken Sie auf den Benutzer, den Sie löschen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
3. Klicken Sie auf "Delete" (Löschen).
4. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).

Ändern der Ansicht der Benutzerliste

Sie können die Anzahl der angezeigten Spalten ändern oder die Reihenfolge der Liste neu sortieren, um die Daten lesefreundlich darzustellen. Siehe Ändern der Listenansicht.

Anzeigen der verbundenen Benutzer

Sie können feststellen, welche Benutzer mit dem EMX-Gerät verbunden sind und welchen Status sie haben. Wenn Sie über Administratorberechtigung verfügen, können Sie die Verbindung jedes Benutzers mit dem EMX-Gerät beenden.

So zeigen Sie verbundene Benutzer an:

1. Wählen Sie "Maintenance" > "Connected Users" (Wartung > Verbundene Benutzer) aus. Das Dialogfeld "Connected Users" (Verbundene Benutzer) wird angezeigt, in dem eine Liste der verbundenen Benutzer mit den folgenden Informationen angezeigt wird:

Spalte	Beschreibung
User Name (Benutzername)	Der von verbundenen Benutzern verwendete Benutzername.
IP Address (IP-Adresse)	IP-Adresse des Hosts des Benutzers. Bei der Anmeldung über eine serielle Verbindung wird statt einer IP-Adresse <local> angezeigt.

Spalte	Beschreibung
Client Type (Clienttyp)	Die Schnittstelle, über die der Benutzer mit der EMX-Einheit verbunden ist. ▪ Web-GUI: Bezieht sich auf die Webschnittstelle von EMX. ▪ CLI: Bezieht sich auf die Befehlszeilenschnittstelle (CLI). Die Informationen in Klammern hinter "CLI" zeigen an, wie dieser Benutzer mit der Befehlszeilenschnittstelle verbunden ist. - *Serial (Seriell)*: Gibt die lokale Verbindung an (seriell oder USB). - *SSH*: Gibt die SSH-Verbindung an. - *Telnet*: Gibt die Telnet-Verbindung an.
Idle Time (Zeit der Inaktivität)	Die Zeitdauer, die ein Benutzer inaktiv ist. Die Einheit "min" stellt Minuten dar.

1. Klicken Sie auf die entsprechende Schaltfläche "Disconnect" (Trennen), um einen Benutzer zu trennen.
   a. Es wird ein Dialogfeld angezeigt, das Sie auffordert, den Vorgang zu bestätigen.
   b. Klicken Sie auf "Yes" (Ja), um den Benutzer zu trennen, oder auf "No" (Nein), um den Vorgang abzubrechen. Wenn Sie auf "Yes" (Ja) klicken, wird der Benutzer gezwungen, sich abzumelden.
2. Sie können die Sortierreihenfolge der Liste bei Bedarf ändern. See Ändern der Sortierreihenfolge.
3. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Verwalten von Benutzerfunktionen

Einrichten von Benutzerfunktionen

Zum Verwalten von Einstellungen müssen Sie sich mit den entsprechenden Berechtigungen beim Benutzerkonto anmelden. Eine Benutzerfunktion definiert die Vorgänge und Funktionen, die ein Benutzer ausführen oder auf die er zugreifen darf. Jedem Benutzer muss mindestens eine Benutzerfunktion zugewiesen werden.

Auf der EMX-Einheit sind zwei Benutzerfunktionen vordefiniert: **Admin** und **Operator**.

- Die Benutzerfunktion "Admin" verfügt über uneingeschränkte Berechtigungen. Sie können diese Benutzerfunktion weder ändern noch löschen.
- Die Benutzerfunktion "Operator" verfügt über eingeschränkte Berechtigungen für häufig verwendete Funktionen. Sie können diese Benutzerfunktion ändern oder löschen. Die Benutzerfunktion "Operator" enthält standardmäßig die folgenden Berechtigungen:
  - Ereigniseinstellungen anzeigen
  - Lokales Ereignisprotokoll anzeigen
  - Ereigniseinstellungen ändern
  - Eigenes Kennwort ändern
  - EMD-Konfiguration ändern
- Die Benutzerfunktion "Operator" wird einem neu erstellten Benutzerprofil standardmäßig zugewiesen. Siehe ***Erstellen von Benutzerprofilen*** (auf Seite 62).

Erstellen einer Benutzerfunktion

Erstellen Sie eine neue Benutzerfunktion, wenn Sie eine neue Kombination an Berechtigungen benötigen.

So erstellen Sie eine Benutzerfunktion:

1. Wählen Sie "User Management" > "Roles" (Benutzerverwaltung > Benutzerfunktionen) aus. Das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) wird angezeigt.

Tipp: Sie können das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) auch aufrufen, indem Sie im Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) auf die Schaltfläche "Manage Roles" (Benutzerfunktionen verwalten) klicken.

2. Klicken Sie auf "New" (Neu). Das Dialogfeld "Create New Role" (Neue Benutzerfunktion erstellen) wird angezeigt.
3. Geben Sie im Feld "Role Name" (Name der Benutzerfunktion) einen Namen ein.
4. Geben Sie im Feld "Description" (Beschreibung) eine Beschreibung für die Benutzerfunktion ein.
5. Klicken Sie auf die Registerkarte "Privileges" (Berechtigungen), um mindestens eine Berechtigung zuzuweisen.
   a. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Privileges to new Role" (Berechtigungen zur neuen Benutzerfunktion hinzufügen) wird angezeigt.
   b. Wählen Sie die gewünschte Berechtigung aus der Liste "Privileges" (Berechtigungen) aus.
   c. Wenn die ausgewählte Berechtigung eine Argumenteinstellung enthält, wird die Liste "Arguments" (Argumente) rechts angezeigt. Wählen Sie anschließend mindestens ein Argument aus.
   d. Klicken Sie auf "Add" (Hinzufügen), um die ausgewählte Berechtigung (und gegebenenfalls Argumente) hinzuzufügen.
   e. Wiederholen Sie die Schritte *a* bis *d*, bis Sie alle erforderlichen Berechtigungen hinzugefügt haben.
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Nun können Sie die neue Benutzerfunktion beliebigen Benutzern zuweisen. Siehe ***Erstellen von Benutzerprofilen*** (auf Seite 62) oder ***Ändern von Benutzerprofilen*** (auf Seite 67).

Ändern von Benutzerfunktionen

Sie können die Einstellungen für eine vorhandene Benutzerfunktion ändern, jedoch nicht den Namen.

So ändern Sie eine Benutzerfunktion:

1. Wählen Sie "User Management" > "Roles" (Benutzerverwaltung > Benutzerfunktionen) aus. Das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) wird angezeigt.

   Tipp: Sie können das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) auch aufrufen, indem Sie im Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) auf die Schaltfläche "Manage Roles" (Benutzerfunktionen verwalten) klicken.

2. Klicken Sie auf die Benutzerfunktion, die Sie ändern möchten.

3. Klicken Sie auf "Edit" (Bearbeiten) oder doppelklicken Sie auf die Benutzerfunktion. Das Dialogfeld "Edit Role 'XXX'" (Benutzerfunktion 'XXX' bearbeiten) wird angezeigt, wobei XXX den Namen der Benutzerfunktion darstellt.

   Tipp: Sie können das Dialogfeld "Edit Role 'XXX'" (Benutzerfunktionen 'XXX' bearbeiten) auch aufrufen, indem Sie im Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) auf die Schaltfläche "Edit Role" (Benutzerfunktionen bearbeiten) klicken.

4. Ändern Sie gegebenenfalls den im Feld "Description" (Beschreibung) angezeigten Text.
5. Klicken Sie auf die Registerkarte "Privileges" (Berechtigungen), um die Berechtigungen zu ändern.

   Hinweis: Die Berechtigungen für die Administrator-Benutzerfunktion können nicht geändert werden.

6. So löschen Sie eine beliebige Berechtigung:
   a. Klicken Sie auf die Berechtigung, die Sie löschen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
   b. Klicken Sie auf "Delete" (Löschen).
7. So fügen Sie eine beliebige Berechtigung hinzu:
   a. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Privileges to Role 'XXX'" (Berechtigungen zu Benutzerfunktion 'XXX' hinzufügen) wird angezeigt, wobei XXX den Namen der Benutzerfunktion darstellt.
   b. Wählen Sie die gewünschte Berechtigung aus der Liste "Privileges" (Berechtigungen) aus.
   c. Wenn die ausgewählte Berechtigung eine Argumenteinstellung enthält, wird die Liste "Arguments" (Argumente) rechts angezeigt. Wählen Sie anschließend mindestens ein Argument aus.
   d. Klicken Sie auf "Add" (Hinzufügen), um die ausgewählte Berechtigung (und gegebenenfalls Argumente) hinzuzufügen.
   e. Wiederholen Sie die Schritte *a* bis *d*, bis Sie alle erforderlichen Berechtigungen hinzugefügt haben.
8. Führen Sie die folgenden Schritte aus, um die Argumente einer bestimmten Berechtigung zu ändern:
   a. Wählen Sie den Berechtigung aus, indem Sie darauf klicken.
   b. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "Edit arguments of privilege 'XXX'" (Argumente der Berechtigung 'XXX' bearbeiten) wird angezeigt, wobei XXX den Namen der Berechtigung darstellt.

Hinweis: Wenn die ausgewählte Berechtigung keine Argumente enthält, ist die Schaltfläche "Edit" (Bearbeiten) deaktiviert.

c. Wählen Sie das gewünschte Argument aus. Sie können mehrere Optionen auswählen.

d. Klicken Sie auf OK.

9. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen einer Benutzerfunktion

Außer der Benutzerfunktion "Admin" können Sie alle Benutzerfunktionen löschen.

So löschen Sie eine Benutzerfunktion:

1. Wählen Sie "User Management" > "Roles" (Benutzerverwaltung > Benutzerfunktionen) aus. Das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) wird angezeigt.

Tipp: Sie können das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) auch aufrufen, indem Sie im Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) auf die Schaltfläche "Manage Roles" (Benutzerfunktionen verwalten) klicken.

2. Klicken Sie auf die Benutzerfunktion, die Sie löschen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
3. Klicken Sie auf "Delete" (Löschen).
4. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).

Kapitel 5 EMX-Geräteverwaltung

In diesem Kapitel

Übersicht....74
Benennen des EMX-Geräts....74
Anzeigen der Geräteinformationen....75
Einstellen von Datum und Uhrzeit....75
Festlegen der Höhe des Geräts über Normal-Null....77
Ändern der Maßeinheiten....78
Festlegen der Anzeige von Elementen in der Verzeichnisstruktur....79
Ändern der Netzwerkkonfiguration....81
Ändern der Netzwerkdiensteinstellungen....89
Konfigurieren der SMTP-Einstellungen....93
Einrichten einer EMX-Einheit mit der Sammelkonfiguration....94
Firmware-Upgrade....96
Netzwerkdiagnose....99
Herunterladen von Diagnoseinformationen....101
Neustart des EMX-Geräts....102
Wiederherstellen der werksseitigen Standardeinstellungen....103

Übersicht

Die folgenden Abschnitte enthalten Informationen zum Einrichten und Verwalten der EMX-Einheit, nachdem das EMX-Gerät installiert wurde.

Wenn Sie bereits eine EMX-Einheit installiert und konfiguriert haben und nun eine andere EMX-Einheit konfigurieren, können Sie die Konfiguration optional mit der Funktion "Bulk Configuration" (Sammelkonfiguration) vereinfachen. Siehe ***Einrichten einer EMX-Einheit mit der Sammelkonfiguration*** (auf Seite 94).

Benennen des EMX-Geräts

Der Standardname für ein EMX-Gerät lautet *EMX*, der bei Bedarf geändert werden kann.

So ändern Sie den Gerätenamen:

1. Klicken Sie im linken Navigationsbereich auf den Ordner "EMX". Die Seite "Settings" (Einstellungen) wird angezeigt.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie auf der Seite "Settings" (Einstellungen) auf "Setup" (Einrichten). Das Dialogfeld "EMX Setup" (EMX einrichten) wird eingeblendet.
3. Geben Sie im Feld "Device Name" (Gerätename) einen neuen Namen ein.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Anzeigen der Geräteinformationen

Im Dialogfeld "Device Information" (Geräteinformationen) werden spezifische Informationen zum EMX-Gerät, auf das Sie zugreifen, angezeigt, z. B. IDs und Protokollversionen der Assetsensoren.

So zeigen Sie Geräteinformationen an:

1. Wählen Sie "Maintenance" > "Device Information" (Wartung > Geräteinformationen) aus. Das Dialogfeld "Device Information" (Geräteinformationen) wird eingeblendet.
2. Klicken Sie auf die Registerkarte mit den Informationen, die Sie anzeigen möchten.

Registerkarte	Angezeigte Informationen
Device Information (Geräteinformationen)	Allgemeine Geräteinformationen, wie z. B. Modellname, Seriennummer, Firmwareversion, Hardwareversion usw.
Asset-Strips	Die ID, Bootversion, Anwendungsversion und Protokollversion jedes Assetsensors.

3. Vergrößern Sie gegebenenfalls das Dialogfeld.
4. Sie können die Liste neu sortieren oder die angezeigten Spalten ändern.
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Tipp: Die Firmwareversion kann auch überprüft werden, indem Sie im Fenster "EMX Explorer" auf den Ordner "EMX" klicken.

Einstellen von Datum und Uhrzeit

Stellen Sie die interne Uhr des EMX-Geräts manuell ein, oder lassen Sie Datum und Uhrzeit für die EMX-Einheit über einen NTP-Server (Network Time Protocol) vorgeben.

So stellen Sie das Datum und die Uhrzeit ein:

1. Wählen Sie "Device Settings" > "Date/Time" (Geräteeinstellungen > Datum/Uhrzeit) aus. Das Dialogfeld "Configure Date/Time Settings" (Datum-/Uhrzeiteinstellungen konfigurieren) wird angezeigt.

2. Klicken Sie im Feld "Time Zone" (Zeitzone) auf die Dropdown-Liste, und wählen Sie die gewünschte Zeitzone aus der Liste aus.
3. Wenn für Ihre Zeitzone die Sommerzeit gilt, vergewissern Sie sich, dass das Kontrollkästchen "Automatic Daylight Saving Time Adjustment" (Automatische Anpassung der Sommerzeit) aktiviert ist.

   Wenn die Regeln für die Sommerzeit nicht für die ausgewählte Zeitzone zur Verfügung stehen, kann das Kontrollkästchen nicht konfiguriert werden.
4. Wählen Sie eine der folgenden Methoden zum Einstellen des Datums und der Uhrzeit:
   - Um Datum und Uhrzeit anzupassen, wählen Sie die Option "User specified time" (Benutzerdefinierte Zeit) aus und geben anschließend das Datum und die Uhrzeit in die entsprechenden Felder ein. Verwenden Sie für das Datum das Format JJJJ-MM-TT und für die Uhrzeit das Format HH:MM:SS.
     - Um das Datum einzustellen, löschen Sie die Zahlen im Feld "Date" (Datum) und geben das neue Datum ein oder klicken auf das Kalendersymbol , um ein Datum auszuwählen.
     - Die Zeit wird im 24-Stunden-Format angezeigt. Geben Sie dementsprechend 13 für 1:00 Uhr nachmittags, 14 für 2:00 Uhr nachmittags usw. ein. Sie können die Zeit eingeben, indem Sie die vorhandenen Zahlen löschen und in die Felder für Stunde, Minute und Sekunden neue Zahlen eingeben oder auf die Pfeile klicken, um jede Zahl auszuwählen.
   - Um Datum und Uhrzeit automatisch über einen NTP-Server einzustellen, wählen Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren). Die NTP-Server können auf zwei Arten zugewiesen werden.

- Um die über DHCP zugewiesenen NTP-Server zu verwenden, müssen Sie sicherstellen, dass das Kontrollkästchen "Always use the servers below and ignore DHCP-provided servers" (Unten angegebene Server immer verwenden und über DHCP zugewiesene Server ignorieren) deaktiviert ist. Diese Methode kann nur verwendet werden, wenn entweder IPv4- oder IPv6-DHCP aktiviert ist.
- Um die manuell angegebenen NTP-Server zu verwenden, aktivieren Sie das Kontrollkästchen "Always use the servers below and ignore DHCP-provided servers" (Unten angegebene Server immer verwenden und über DHCP zugewiesene Server ignorieren), und geben Sie den primären NTP-Server im Feld "First Time Server" (Primärer Server) an. Ein sekundärer NTP-Server ist optional.

Hinweis: Wenn die IP-Adresse des EMX-Geräts über IPv4- oder IPv6-DHCP zugewiesen wird, können die NTP-Server automatisch erkannt werden. In diesem Fall werden die Daten überschrieben, die Sie in die Felder für den primären und den sekundären Zeitserver eingegeben haben.

5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Festlegen der Höhe des Geräts über Normal-Null

Sie müssen die Höhe des EMX-Geräts über dem Meeresspiegel angeben, wenn ein Differenzluftdrucksensor von Raritan angeschlossen ist. Dies liegt daran, dass die Höhe des Geräts mit dem Höhenkorrekturfaktor in Zusammenhang steht. Siehe ***Höhenkorrekturfaktoren*** (siehe "***Faktoren zur Höhenkorrektur (EMX)***" auf Seite 341).

Die Standardmaßeinheit für die Höhenangabe ist Meter. Sie können bei der Maßeinheit je nach Benutzerberechtigung zwischen Meter und Fuß wechseln. Siehe ***Ändern der Maßeinheiten*** (auf Seite 78).

So geben Sie die Höhe des EMX-Geräts über Normal-Null an:

1. Klicken Sie im linken Navigationsbereich auf den Ordner "EMX". Die Seite "Settings" (Einstellungen) wird angezeigt.

Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie auf der Seite "Settings" (Einstellungen) auf "Setup" (Einrichten). Das Dialogfeld "EMX Setup" (EMX einrichten) wird eingeblendet.
3. Geben Sie im Feld "Altitude" (Höhe) eine Ganzzahl ein. Je nach der angezeigten Maßeinheit unterscheidet sich der Bereich der zulässigen Zahlen.

- Für Meter (m) reicht der Wertebereich von 0 bis 3000.
- Für Fuß (ft) reicht der Wertebereich von 0 bis 9842.

4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern der Maßeinheiten

Die folgenden Maßeinheiten gelten standardmäßig für alle Daten, die in der EMX-Webschnittstelle angezeigt werden:

- Temperatur: Grad Celsius (°C)
- Länge oder Höhe: Meter (m)
- Luftdruck: Pascal (pa)

Die EMX-Webschnittstelle ermöglicht die Verwendung verschiedener Maßeinheiten auf der Grundlage des Anmeldenamens für den Benutzer. Das bedeutet, dass bei verschiedenen Benutzern entsprechend ihren Einstellungen unterschiedliche Maßeinheiten angezeigt werden. Für die einzelnen Maßeinheiten gibt es folgende Alternativen:

- Temperatur: Grad Fahrenheit (°F)
- Länge oder Höhe: Fuß (ft)
- Luftdruck: psi

Legen Sie die gewünschte Maßeinheit beim Erstellen von Benutzerprofilen fest. Siehe ***Erstellen von Benutzerprofilen*** (auf Seite 62). Um die Einstellung für die Maßeinheit ändern zu können, müssen Sie über Administratorrechte verfügen.

So richten Sie die bevorzugten Maßeinheiten ein:

1. Wählen Sie "User Management" > "Users" (Benutzerverwaltung > Benutzer) aus. Das Dialogfeld "Manage Users" (Benutzer verwalten) wird angezeigt.
2. Wählen Sie den Benutzer aus, indem Sie auf ihn klicken.
3. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf den Benutzer. Das Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) wird angezeigt, wobei XXX den Benutzernamen darstellt.
4. Klicken Sie auf die Registerkarte "Preferences" (Einstellungen).
5. Um die Temperatureinheit zu ändern, wählen Sie die gewünschte Option im Feld "Temperature Unit" (Temperatureinheit).
   - °C: Mit dieser Option wird die Temperatur in Celsius angezeigt.
   - °F: Mit dieser Option wird die Temperatur in Fahrenheit angezeigt.
6. Um die Einheit für die Länge oder die Höhe zu ändern, wählen Sie die gewünschte Option im Feld "Length Unit" (Längeneinheit).

- Meter: Mit dieser Option wird die Länge oder Höhe in Meter angezeigt.
- Feet (Fuß): Mit dieser Option wird die Länge oder Höhe in Fuß angezeigt.

7. Um die Druckeinheit zu ändern, wählen Sie die gewünschte Option im Feld "Pressure Unit" (Druckeinheit).
   - Pascal: Mit dieser Option wird der Druckwert in Pascal (Pa) angezeigt. Ein Pascal entspricht 1 Newton pro Quadratmeter.
   - psi: Mit dieser Option wird der Druckwert in psi angezeigt. Psi steht für Pounds per Square Inch (Pfund pro Quadratzoll).
8. Klicken Sie auf "OK", um die Änderungen zu speichern.

Festlegen der Anzeige von Elementen in der Verzeichnisstruktur

Die EMX-Webschnittstelle zeigt angeschlossene Geräte standardmäßig nur dann in der Verzeichnisstruktur an, wenn Geräte physisch an die FEATURE- und RS-485-Ports (Zusatz-Ports) angeschlossen sind. Wenn keine Geräte angeschlossen sind, wird nichts angezeigt.

Mit der EMX-Webschnittstelle können Sie festlegen, wann und wie Symbole für angeschlossene und nicht angeschlossene Geräte in der Verzeichnisstruktur angezeigt werden.

Anzeigen von Assetsensoren

Angeschlossene Assetsensoren lassen sich auf zwei Arten in der Verzeichnisstruktur der Webschnittstelle anzeigen:

- Assetsensoren werden nur angezeigt, wenn sie physisch angeschlossen sind.
- Assetsensoren werden immer angezeigt, unabhängig davon, ob sie physisch angeschlossen sind oder nicht; das Aussehen ihrer Symbole ändert sich jedoch, um auf den Verbindungsstatus hinzuweisen.

So legen Sie fest, wie angeschlossene Assetsensoren angezeigt werden:

1. Klicken Sie auf den Ordner "Feature Ports" (Feature-Ports). Die Seite "Feature Ports" (Feature-Ports) wird im rechten Fensterbereich mit einer Liste aller FEATURE-Ports geöffnet.
2. Wählen Sie die Nummer des Ports aus, den Sie konfigurieren möchten, und klicken Sie auf "Setup" (Einrichtung). Sie können auch auf die Port-Nummer doppelklicken. Das Dialogfeld "Feature Port Setup" (Feature-Port einrichten) für den ausgewählten Port wird angezeigt.
3. Wählen Sie im Feld "Detection Mode" (Erkennungsmodus), wie die angeschlossenen Assetsensoren angezeigt werden sollen.

- Disabled (Deaktiviert): Wenn aktiviert, wird der Port deaktiviert, und an den Port angeschlossene Geräte werden nicht erkannt.
- Auto (Automatisch): Für diesen Port wird nur ein Symbol angezeigt, wenn das EMX-Gerät die physische Verbindung des Assetsensors an diesem Port erkennt. Andernfalls wird nichts angezeigt. Dies ist die Standardmethode.
- Pinned (Anheften): Für diesen Port wird immer ein Symbol angezeigt, das Symbol variiert jedoch entsprechend dem Verbindungsstatus. Wird die Verbindung eines Assetsensors an einem bestimmten Feature-Port erkannt, wird das Symbol für diesen Port angezeigt. Falls nicht, wird stattdessen das Symbol eingeblendet. Siehe ***Festlegen der Anzeige von Elementen der Verzeichnisstruktur*** (siehe "***Festlegen der Anzeige von Elementen in der Verzeichnisstruktur***" auf Seite 79).

  Wenn das Kontrollkästchen "Pinned" (Anheften) aktiviert ist, klicken Sie auf den Dropdown-Pfeil, um den anzuzeigenden Gerätetyp auszuwählen. Wählen Sie "Asset Strip" für Assetsensoren.

4. Klicken Sie auf "OK", um die Änderungen zu speichern.

In der Verzeichnisstruktur steht hinter dem Symbol, falls vorhanden, der Gerätename (sofern verfügbar), der Gerätetyp und die Port-Nummer.

Anzeigen von LHX-Wärmetauschern

Angeschlossene Schroff® LHX-Wärmetauscher lassen sich in der Verzeichnisstruktur der Webschnittstelle auf zwei Arten anzeigen:

- LHX-Wärmetauscher werden nur angezeigt, wenn sie physisch angeschlossen sind.
- LHX-Wärmetauscher werden immer angezeigt, unabhängig davon, ob sie physisch angeschlossen sind oder nicht; das Aussehen ihrer Symbole ändert sich jedoch, um auf den Verbindungsstatus hinzuweisen.

Die EMX-Einheit unterstützt die Modelle LHX-20 und LHX-40.

Hinweis: Die Unterstützung für den Schroff LHX muss aktiviert sein, damit der LHX angezeigt werden kann. Siehe **Aktivieren und Deaktivieren der Unterstützung für Schroff LHX-Wärmetauscher** *(auf Seite 210).*

So legen Sie fest, wie angeschlossene LHX-Wärmetauscher angezeigt werden:

1. Abhängig vom Port, an den Sie den Sensor anschließen möchten, klicken Sie auf den Ordner "Auxiliary Ports" (Zusätzliche Ports) oder "Feature Ports".

2. Wählen Sie die Nummer des Ports aus, den Sie konfigurieren möchten, und klicken Sie auf "Setup" (Einrichtung). Sie können auch auf die Port-Nummer doppelklicken. Das Dialogfeld "Auxiliary Port Setup" (Zusätzlichen Port einrichten) für den ausgewählten Port wird angezeigt.
3. Wählen Sie im Feld "Detection Mode" (Erkennungsmodus), wie angeschlossene LHX-Wärmetauscher angezeigt werden sollen.
   - Disabled (Deaktiviert): Wenn aktiviert, wird der Port deaktiviert, und an den Port angeschlossene Geräte werden nicht erkannt.
   - Auto (Automatisch): Für diesen Port wird nur ein Symbol angezeigt, wenn das EMX-Gerät die physische Verbindung des LHX-Wärmetauschers an diesem Port erkennt. Andernfalls wird nichts angezeigt. Dies ist die Standardmethode.
   - Pinned (Anheften): Für diesen Port wird immer ein Symbol angezeigt, das Symbol variiert jedoch entsprechend dem Verbindungsstatus. Siehe ***Gerätestatus und Symbolwechsel*** (auf Seite 214).

     Wenn das Kontrollkästchen "Pinned" (Anheften) aktiviert ist, klicken Sie auf den Dropdown-Pfeil, um den entsprechenden Gerätetyp für diesen Port auszuwählen. LHX 20 oder LHX 40.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

In der Verzeichnisstruktur steht hinter dem Symbol, falls vorhanden, der Gerätename (sofern verfügbar), der Gerätetyp und die Port-Nummer oder der FEATURE-Port (sofern zutreffend).

Ändern der Netzwerkkonfiguration

Zu den Netzwerkeinstellungen, die Sie über die Webschnittstelle ändern können, gehören die Einstellungen "drahtgebunden", "drahtlos" IPv4 und IPv6.

Ändern der Netzwerkschnittstelleneinstellungen

Die EMX-Einheit unterstützt zwei Typen von Netzwerkschnittstellen: drahtgebundene und drahtlose. Sie sollte die Einstellungen für die Netzwerkschnittstellen entsprechend des zutreffenden Netzwerkmodus konfigurieren. Siehe ***Anschließen der EMX-Einheit an das Netzwerk*** (auf Seite 13).

Drahtgebundene Netzwerkeinstellungen

Die Einstellungen der LAN-Schnittstelle (Geschwindigkeit und Duplex-Modus) wurden während der Installation und Konfiguration festgelegt. Siehe Erstkonfiguration des Netzwerks.

Standardmäßig sind die LAN-Geschwindigkeit und der Duplex-Modus auf "Auto" (Automatisch) eingestellt. Diese Einstellung kann für fast alle Szenarien verwendet werden. Sie können die Einstellung ändern, wenn spezielle lokale Anforderungen erfüllt werden müssen.

So ändern Sie die Netzwerkschnittstelleneinstellungen:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Das Dialogfeld "Network Configuration" (Netzwerkkonfiguration) wird angezeigt.
2. Die Registerkarte "Interface Settings" (Schnittstelleneinstellungen) sollte ausgewählt sein. Falls nicht, klicken Sie auf die Registerkarte "Interface Settings" (Schnittstelleneinstellungen).
3. Klicken Sie im Feld "Network Interface" (Netzwerkschnittstelle) auf die Dropdown-Liste, und wählen Sie "Wired" (Verkabelt) aus der Liste aus.
4. Um die LAN-Geschwindigkeit zu ändern, klicken Sie in der Dropdown-Liste auf das Feld "Speed" (Geschwindigkeit) und wählen eine Option aus der Liste aus.
   - Auto (Automatisch): Das System legt die optimale LAN-Geschwindigkeit mithilfe der automatischen Aushandlung fest.
   - 10 Mbit/s: Die LAN-Geschwindigkeit beträgt immer 10 Mbps.
   - 100 Mbit/s: Die LAN-Geschwindigkeit beträgt immer 100 Mbps.
5. Um den Duplex-Modus zu ändern, klicken Sie in der Dropdown-Liste auf das Feld "Duplex" und wählen eine Option aus der Liste aus.
   - Auto (Automatisch): Die EMX-Einheit wählt den optimalen Übertragungsmodus mithilfe der automatischen Aushandlung aus.
   - Full (Voll): Daten werden gleichzeitig in beide Richtungen übertragen.
   - Half (Halb): Daten werden jeweils in eine Richtung übertragen (zu oder von EMX).
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Tipp: Sie können den LAN-Status im Feld "Current State" (Aktueller Status) überprüfen, einschließlich Geschwindigkeit und Duplex-Modus.

Drahtlose Netzwerkeinstellungen

Die drahtlosen SSID-, PSK und BSSID-Parameter wurden während der Installation und Konfiguration festgelegt. Siehe Erstkonfiguration des Netzwerks. Sie können sie über die Webschnittstelle ändern.

So ändern Sie die Drahtlosschnittstelleneinstellungen:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Das Dialogfeld "Network Configuration" (Netzwerkkonfiguration) wird angezeigt.
2. Die Registerkarte "Interface Settings" (Schnittstelleneinstellungen) sollte ausgewählt sein. Falls nicht, klicken Sie auf die Registerkarte "Interface Settings" (Schnittstelleneinstellungen).
3. Klicken Sie im Feld "Network Interface" (Netzwerkschnittstelle) auf die Dropdown-Liste, und wählen Sie "Wireless" (Drahtlos) aus der Liste aus.
4. Prüfen Sie das Feld "Hardware State" (Hardwarestatus), um sicherzustellen, dass das EMX-Gerät einen drahtlosen USB LAN-Adapter erkannt hat. Falls nicht, prüfen Sie, ob der USB LAN-Adapter fest verbunden ist und unterstützt wird. Siehe ***Anschließen der EMX-Einheit an das Netzwerk*** (auf Seite 13).
5. Geben Sie den Namen des drahtlosen Access Point (AP) in das Feld "SSID" ein.
6. Wenn die BSSID verfügbar ist, markieren Sie das Kontrollkästchen "Force AP BSSID" (AP BSSID erzwingen) und geben Sie die MAC-Adresse in das Feld "BSSID" ein.

   Hinweis: BSSID bezieht sich auf die MAC-Adresse eines Access Point im drahtlosen Netzwerk.

7. Klicken Sie im Feld "Authentication" (Authentifizierung) auf den Dropdown-Pfeil, und wählen Sie eine geeignete Option aus der Liste aus.

Option	Beschreibung
No Authentication (Keine Authentifizierung)	Wählen Sie diese Option, wenn keine Authentifizierungdaten erforderlich sind.
PSK	Für diese Option ist ein Pre-Shared Key (vorher vereinbarter Schlüssel) erforderlich. ▪ Geben Sie in das Feld "Pre-Shared Key" den PSK-String ein.

Option	Beschreibung
EAP - PEAP	PEAP steht für "Protected Extensible Authentication Protocol" (Geschütztes erweiterbares Authentifizierungsprotokoll). Die folgenden Authentifizierungsdaten sind erforderlich: ▪ Inner Authentication (Innere Authentifizierung): Es wird nur Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) unterstützt, mit dem die Authentifizierung bei Datenbanken ermöglicht wird, die MSCHAPv2 unterstützen. ▪ Identity (Identität): Geben Sie Ihren Benutzername für die EAP-Authentifizierung ein. ▪ Password (Kennwort): Geben Sie Ihr Kennwort für die EAP-Authentifizierung ein. ▪ CA Certificate (CA-Zertifikat): Für die EAP-Authentifizierung muss ein externes CA-Zertifikat bereitgestellt werden. Klicken Sie auf "Browse" (Durchsuchen), um eine gültige Zertifikatdatei auszuwählen. - Um den Inhalt der ausgewählten Zertifikatdatei anzuzeigen, klicken Sie auf "Show" (Anzeigen). - Wenn das ausgewählte Zertifikat ungültig ist, klicken Sie auf "Remove" (Entfernen). Wählen Sie anschließend eine neue Datei aus.

1. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern der Netzwerkeinstellungen

Die EMX-Einheit wurde während der Installation und Konfiguration für die Verbindung mit einem Netzwerk konfiguriert. Siehe ***Konfigurieren der EMX-Einheit*** (auf Seite 11). Bei Bedarf können Sie die Netzwerkeinstellungen mithilfe der Webschnittstelle ändern.

Auswahl des Internetprotokolls

Das EMX-Gerät unterstützt zwei Typen von Internetprotokollen -- IPv4 und IPv6. Sie können ein oder beide Internetprotokoll(e) aktivieren. Nachdem die gewünschten Internetprotokolle aktiviert wurden, entsprechen die folgenden Protokolle, jedoch nicht nur diese, den aktivierten Internetprotokollen:

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

So wählen Sie das geeignete Internetprotokoll aus:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Das Dialogfeld "Network Configuration" (Netzwerkkonfiguration) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IP Protocol" (IP-Protokoll).
3. Markieren Sie ein Kontrollkästchen entsprechend der Internetprotokolle, die Sie aktivieren möchten:
   - IPv4 only (Nur IPv4): Aktiviert "IPv4 only" (Nur IPv4) an allen Schnittstellen. Dies ist die Standardeinstellung.
   - IPv6 only (Nur IPv6): Aktiviert "IPv6 only" (Nur IPv6) an allen Schnittstellen.
   - IPv4 and IPv6 (IPv4 und IPv6): Aktiviert IPv4 und IPv6 an allen Schnittstellen.
4. Wenn Sie im vorherigen Schritt das Kontrollkästchen "IPv4 and IPv6" (IPv4 und IPv6) markiert haben, müssen Sie festlegen, welche IP-Adresse verwendet wird, wenn der DNS-Resolver die IPv4- und die IPv6-Adresse zurückgibt.
   - IPv4 Address (IPv4-Adresse): Verwenden Sie die vom DNS-Server zurückgegebenen IPv4-Adressen.
   - IPv6 Address (IPv6-Adresse): Verwenden Sie die vom DNS-Server zurückgegebenen IPv6-Adressen.
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern der IPv4-Einstellungen

Sie müssen das IPv4-Protokoll aktiviert haben, bevor Sie die IPv4-Netzwerkeinstellungen ändern können. Siehe ***Auswahl des Internetprotokolls*** (auf Seite 85).

So ändern Sie die IPv4-Einstellungen:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Das Dialogfeld "Network Configuration" (Netzwerkkonfiguration) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4 Settings" (IPv4-Einstellungen).
3. Klicken Sie im Feld "IP Auto Configuration" (Automatische IP-Konfiguration) auf die Dropdown-Liste, und wählen Sie die gewünschte Option aus der Liste aus.

Option	Beschreibung
DHCP	Um die EMX-Einheit automatisch zu konfigurieren, wählen Sie "DHCP" aus. Wenn DHCP aktiviert ist, können Sie einen bevorzugten DHCP-Host-Namen eingeben (optional). Geben Sie im Feld "Preferred Hostname" (Bevorzugter Hostname) den Hostnamen ein. Der Hostname: ▪ Besteht aus alphanumerischen Zeichen und/oder Bindestrichen ▪ Darf nicht mit einem Bindestrich beginnen oder enden ▪ Darf nicht mehr als 63 Zeichen enthalten ▪ Darf keine Interpunktionszeichen, Leerzeichen und andere Symbole enthalten Aktivieren Sie gegebenenfalls das Kontrollkästchen "Specify DNS server manually" (DNS-Server manuell angeben). Geben Sie anschließend im Feld "Primary DNS Server" (Primärer DNS-Server) die Adresse des primären DNS-Servers ein. Der sekundäre DNS-Server und das DNS-Suffix sind optional.
Static (Statisch)	Um eine IP-Adresse manuell zuzuweisen, wählen Sie "Static" (Statisch) aus und geben die folgenden Informationen in die entsprechenden Felder ein: ▪ IP-Adresse

Option	Beschreibung
	▪ Netzmaske ▪ Gateway ▪ Primärer DNS-Server ▪ Sekundärer DNS-Server (optional) ▪ DNS-Suffix (optional)

4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Hinweis: Die EMX-Einheit unterstützt maximal 3 DNS-Server. Wenn zwei IPv4-DNS-Server und zwei IPv6-DNS-Server zur Verfügung stehen, verwendet die EMX-Einheit nur die primären IPv4- und IPv6-DNS-Server.

Ändern der IPv6-Einstellungen

Sie müssen das IPv6-Protokoll aktiviert haben, bevor Sie die IPv6-Netzwerkeinstellungen ändern können. Siehe ***Auswahl des Internetprotokolls*** (auf Seite 85).

So ändern Sie die IPv6-Einstellungen:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Das Dialogfeld "Network Configuration" (Netzwerkkonfiguration) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv6 Settings" (IPv6-Einstellungen).
3. Klicken Sie im Feld "IP Auto Configuration" (Automatische IP-Konfiguration) auf die Dropdown-Liste, und wählen Sie die gewünschte Option aus der Liste aus.

Option	Beschreibung
Automatic (Automatisch)	Um EMX automatisch zu konfigurieren, wählen Sie "Automatic" (Automatisch) aus. Wenn diese Option aktiviert ist, können Sie einen bevorzugten Host-Namen eingeben (optional). Geben Sie im Feld "Preferred Hostname" (Bevorzugter Hostname) den Hostnamen ein. Der Hostname: ▪ Besteht aus alphanumerischen Zeichen und/oder Bindestrichen ▪ Darf nicht mit einem Bindestrich beginnen oder enden

Option	Beschreibung
	▪ Darf nicht mehr als 63 Zeichen enthalten ▪ Darf keine Interpunktionszeichen, Leerzeichen und andere Symbole enthalten Aktivieren Sie gegebenenfalls das Kontrollkästchen "Specify DNS server manually" (DNS-Server manuell angeben). Geben Sie anschließend im Feld "Primary DNS Server" (Primärer DNS-Server) die Adresse des primären DNS-Servers ein. Der sekundäre DNS-Server und das DNS-Suffix sind optional.
Static (Statisch)	Um eine IP-Adresse manuell zuzuweisen, wählen Sie "Static" (Statisch) aus und geben die folgenden Informationen in die entsprechenden Felder ein: ▪ IP-Adresse ▪ Gateway ▪ Primärer DNS-Server ▪ Sekundärer DNS-Server (optional) ▪ DNS-Suffix (optional)

4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Hinweis: Die EMX-Einheit unterstützt maximal 3 DNS-Server. Wenn zwei IPv4-DNS-Server und zwei IPv6-DNS-Server zur Verfügung stehen, verwendet die EMX-Einheit nur die primären IPv4- und IPv6-DNS-Server.

Funktion eines DNS-Servers

Da die Internetkommunikation auf IP-Adressen basiert, sind entsprechende DNS-Servereinstellungen erforderlich, um Domänennamen (Hostnamen) den entsprechenden IP-Adressen zuzuordnen. Andernfalls kann die EMX-Einheit unter Umständen keine Verbindung zum angegebenen Host herstellen.

Daher sind die DNS-Servereinstellungen für die LDAP-Authentifizierung wichtig. Mit den entsprechenden DNS-Einstellungen kann die EMX-Einheit den Namen des LDAP-Servers für eine IP-Adresse auflösen, um eine Verbindung herzustellen. Wenn die *SSL-Verschlüsselung* aktiviert ist, sind die DNS-Servereinstellungen wichtig, weil nur ein vollständig qualifizierter Domänenname für die Angabe des LDAP-Servers verwendet werden kann.

Für weitere Informationen zur LDAP-Authentifizierung siehe ***Einrichten der LDAP-Authentifizierung*** (auf Seite 129).

Ändern der Netzwerkdiensteinstellungen

Die EMX-Einheit unterstützt die folgenden Netzwerkkommunikationsdienste: HTTPS, HTTP, Telnet und SSH.

HTTPS und HTTP ermöglichen den Zugriff auf die Webschnittstelle, und Telnet und SSH ermöglichen den Zugriff auf die Befehlszeilenschnittstelle.

Standardmäßig ist SSH aktiviert, Telnet deaktiviert und alle TCP-Ports für unterstützte Dienste sind auf Standardports festgelegt. Sie können die Standardeinstellungen gegebenenfalls ändern.

Hinweis: Der Telnet-Zugriff ist standardmäßig deaktiviert, weil die Kommunikation offen stattfindet und daher nicht sicher ist.

Die EMX-Einheit unterstützt auch das SNMP-Protokoll.

Ändern der HTTP(S)-Einstellungen

HTTPS verwendet zum Verschlüsseln des gesamten Verkehrs an das und vom EMX-Gerät die SSL-Technologie (Secure Sockets Layer) und ist somit ein sichereres Protokoll als HTTP.

Standardmäßig wird der Zugriff auf das EMX-Gerät über HTTP automatisch an HTTPS umgeleitet. Siehe ***Erzwingen der HTTPS-Verschlüsselung*** (auf Seite 104).

So ändern Sie die HTTP- oder HTTPS-Porteinstellungen:

1. Wählen Sie "Device Settings" > "Network Services" > "HTTP" (Geräteeinstellungen > Netzwerkdienste > HTTP) aus. Das Dialogfeld "HTTP Settings" (HTTP-Einstellungen) wird angezeigt.
2. Um einen anderen Port für HTTP oder HTTPS zu verwenden, geben Sie eine neue Portnummer in das entsprechende Feld ein. Der gültige Bereich liegt zwischen 1 und 65535.

   Warnung: Unterschiedliche Netzwerkdienste können denselben TCP-Port nicht gemeinsam verwenden.
3. Klicken Sie auf "OK", um die Änderungen zu speichern.

Konfigurieren der SNMP-Einstellungen

Sie können die SNMP-Kommunikation zwischen einem SNMP-Manager und dem EMX-Gerät aktivieren oder deaktivieren. Durch eine Aktivierung der SNMP-Kommunikation kann der Manager den Status des EMX-Geräts abrufen.

Zudem müssen Sie das SNMP-Ziel konfigurieren, wenn die integrierte System-SNMP-Trap-Regel aktiviert ist und das Trap-Ziel noch nicht festgelegt wurde. Siehe ***Ereignisregeln und Aktionen*** (auf Seite 137).

So konfigurieren Sie die SNMP-Kommunikation:

1. Wählen Sie "Device Settings" > "Network Services" > "SNMP" (Geräteeinstellungen > Netzwerkdienste > SNMP) aus. Das Dialogfeld "SNMP Settings" (SNMP-Einstellungen) wird angezeigt.
2. Geben Sie die Informationen zum Trap-Ziel ein, die auf einen oder beide Trap-Typen zutreffen.
3. Navigieren Sie zur gewünschten MIB, und laden Sie sie herunter. Die SNMP-MIB für die EMX-Einheit wird vom SNMP-Manager verwendet.
4. Klicken Sie auf OK.

Ändern der SSH-Einstellungen

Sie können den SSH-Zugriff auf die Befehlszeilenschnittstelle aktivieren oder deaktivieren oder den Standard-TCP-Port für den SSH-Dienst ändern. Darüber hinaus können Sie entscheiden, ob Sie sich entweder mit dem Kennwort oder mit dem öffentlichen Schlüssel über die SSH-Verbindung anmelden.

So ändern Sie die SSH-Diensteinstellungen:

1. Wählen Sie "Device Settings" > "Network Services" > "SSH" (Geräteeinstellungen > Netzwerkdienste > SSH) aus. Das Dialogfeld "SSH Settings" (SSH-Einstellungen) wird angezeigt.
2. Um einen anderen Port zu verwenden, geben Sie eine neue Portnummer in das Feld ein. Der gültige Bereich liegt zwischen 1 und 65535.
3. Zum Aktivieren der SSH-Anwendung wählen Sie das Kontrollkästchen "Enable SSH" (SSH aktivieren) aus. Zum Deaktivieren wählen Sie das Kontrollkästchen ab.
4. Um eine andere Authentifizierungsmethode zu wählen, aktivieren Sie eines der Kontrollkästchen.
   - Allow password authentication only (Nur Kennwortauthentifizierung zulassen): Aktiviert nur die kennwortbasierte Anmeldung.

- Allow public key authentication only (Nur Authentifizierung mit öffentlichem Schlüssel zulassen): Aktiviert nur die Anmeldung auf Basis eines öffentlichen Schlüssels.
- Allow password and public key authentication (Authentifizierung mit Kennwort und öffentlichem Schlüssel zulassen): Aktiviert sowohl die Anmeldung auf Kennwortbasis als auch auf Basis des öffentlichen Schlüssels. Dies ist die Standardeinstellung.

5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Wenn die Authentifizierung mit öffentlichem Schlüssel ausgewählt ist, müssen Sie für jedes Benutzerprofil einen gültigen öffentlichen SSH-Schlüssel eingeben, um sich über die SSH-Verbindung anmelden zu können. Siehe ***Erstellen von Benutzerprofilen*** (auf Seite 62).

Ändern der Telnet-Einstellungen

Sie können den Telnet-Zugriff auf die Befehlszeilenschnittstelle aktivieren oder deaktivieren oder den Standard-TCP-Port für den Telnet-Dienst ändern.

So ändern Sie die Telnet-Diensteinstellungen:

1. Wählen Sie "Device Settings" > "Network Services" > "Telnet" (Geräteeinstellungen > Netzwerkdienste > Telnet) aus. Das Dialogfeld "Telnet Settings" (Telnet-Einstellungen) wird angezeigt.
2. Um einen anderen Port zu verwenden, geben Sie eine neue Portnummer in das Feld ein. Der gültige Bereich liegt zwischen 1 und 65535.
3. Um die Telnet-Anwendung zu aktivieren, wählen Sie das Kontrollkästchen "Enable Telnet Access" (Telnet-Zugriff aktivieren) aus. Zum Deaktivieren wählen Sie das Kontrollkästchen ab.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Aktivieren der Dienstbekanntmachung

Die EMX-Einheit macht alle Dienste bekannt, die über das IP-Netzwerk erreichbar sind. Diese Funktion verwendet DNS-SD (Domain Name System-Service Discovery) und mDNS (multicast DNS). Die bekanntgegebenen Dienste werden von Clients erkannt, auf denen DNS-SD und mDNS implementiert ist.

Es werden unter anderem folgende Dienste bekanntgegeben:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

Diese Funktion ist standardmäßig aktiviert.

So aktivieren Sie die Dienstbekanntmachung:

1. Klicken Sie auf "Device Settings" > "Network Services" > "Service Advertisement" (Geräteeinstellungen > Netzwerkdienste > Dienstbekanntmachung).
2. Klicken Sie im Bestätigungsdialogfeld "Changing Service Advertisement" (Dienstbekanntmachung ändern) auf "Yes" (Ja). Die Funktion wird aktiviert, und das Kontrollkästchen "Service Advertisement" (Dienstbekanntmachung) ist im Menü aktiviert.

So deaktivieren Sie die Dienstbekanntmachung:

1. Klicken Sie auf "Device Settings" > "Network Services" > "Service Advertisement" (Geräteeinstellungen > Netzwerkdienste > Dienstbekanntmachung).
2. Klicken Sie im Bestätigungsdialogfeld "Changing Service Advertisement" (Dienstbekanntmachung ändern) auf "No" (Nein). Die Funktion wird deaktiviert, und das Kontrollkästchen "Service Advertisement" (Dienstbekanntmachung) ist im Menü deaktiviert.

Konfigurieren der SMTP-Einstellungen

Die EMX-Einheit kann so konfiguriert werden, dass Warnungen oder Ereignismeldungen per E-Mail an einen bestimmten Administrator gesendet werden. Dazu müssen Sie die SMTP-Einstellungen konfigurieren, eine IP-Adresse für den SMTP-Server und eine E-Mail-Adresse des Senders eingeben.

Hinweis: Informationen zum Erstellen von Ereignisregeln zum Senden von E-Mail-Benachrichtigungen finden Sie unter **Konfigurieren von Ereignisregeln** *(siehe "***Ereignisregeln und Aktionen***" auf Seite 137).*

So stellen Sie die SMTP-Servereinstellungen ein:

1. Wählen Sie "Device Settings" > "SMTP Server" (Geräteeinstellungen > SMTP-Server) aus. Das Dialogfeld "SMTP Server Settings" (SMTP-Servereinstellungen) wird angezeigt.
2. Geben Sie im Feld "Server Name" (Servername) den Namen oder die IP-Adresse des Mail-Servers ein.
3. Geben Sie im Feld "Port" die Port-Nummer für den SMTP-Server ein. Der Standardwert lautet 25.
4. Geben Sie im Feld "Sender Email Address" (E-Mail-Adresse des Absenders) eine E-Mail-Adresse für den Absender ein.
5. Geben Sie im Feld "Number of Sending Retries" (Anzahl der Senden-Neuversuche) die Anzahl der möglichen Neuversuche für E-Mails ein. Der Standardwert lautet 2 Neuversuche.
6. Geben Sie in das Feld "Time Interval Between Sending Retries (in minutes)" (Zeitintervall zwischen Sende-Neuversuchen [in Minuten]) das Zeitintervall für die Neuversuche zum Senden von E-Mails ein. Die Zeit wird in Minuten gemessen. Der Standardwert lautet 2 Minuten.
7. Führen Sie die folgenden Schritte aus, wenn für den SMTP-Server eine Kennwortauthentifizierung erforderlich ist:
   a. Aktivieren Sie das Kontrollkästchen "Server Requires Authentication" (Authentifizierung für Server erforderlich).
   b. Geben Sie im Feld "User Name" (Benutzername) einen Benutzernamen ein.
   c. Geben Sie im Feld "Password" (Kennwort) ein Kennwort ein.
8. Nachdem Sie die SMTP-Einstellungen konfiguriert haben, können Sie sie testen, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Führen Sie Folgendes aus:
   a. Geben Sie im Feld "Recipient Email Addresses" (E-Mail-Adressen des Empfängers) die E-Mail-Adresse des Empfängers ein. Trennen Sie mehrere E-Mail-Adressen durch Kommata voneinander.

b. Klicken Sie auf "Send Test Email" (Test-E-Mail senden).

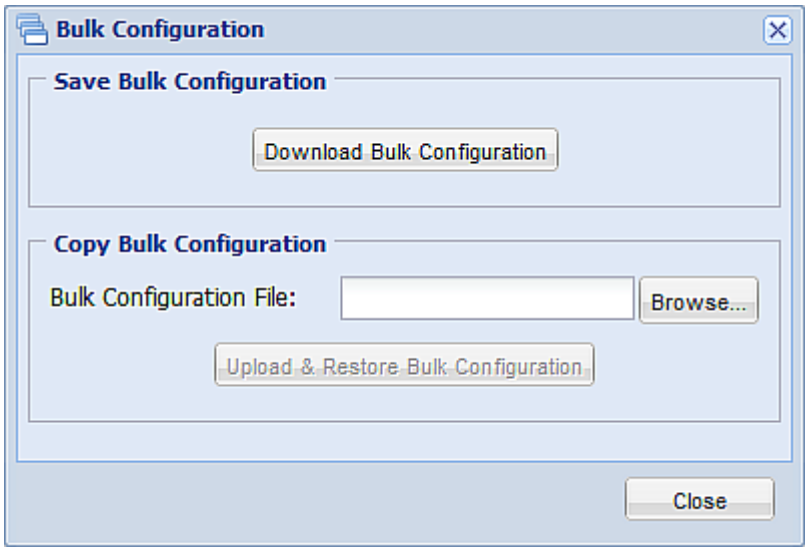
9. Klicken Sie auf "OK", um die Änderungen zu speichern.
10. Prüfen Sie, ob der Empfänger die E-Mail erhält.

Einrichten einer EMX-Einheit mit der Sammelkonfiguration

Verwenden Sie diese Funktion, wenn Sie bereits eine EMX-Einheit eingerichtet haben und nun eine weitere einrichten möchten. Mit dem Feature "Bulk Configuration" (Sammelkonfiguration) können Sie die Einstellungen eines konfigurierten EMX-Geräts auf dem PC speichern. Sie können diese Konfigurationsdatei für Folgendes verwenden:

- Kopieren Sie diese Konfiguration für andere EMX-Geräte desselben Modells und derselben Firmwareversion.
- Setzen Sie die Einstellungen desselben EMX-Geräts auf die vorherige Konfiguration zurück.

Um die EMX-Konfigurationen speichern und kopieren zu können, benötigen Sie Administratorberechtigung.



Speichern einer EMX-Konfiguration

Ein Quellgerät ist ein bereits konfiguriertes EMX-Gerät, das zum Erstellen einer Konfigurationsdatei verwendet wird. Diese Datei enthält die Einstellungen, die für alle >ProductName<-Geräte gemeinsam verwendet werden können. Diese Einstellungen umfassen Benutzer- und Rollenkonfigurationen, Ereignisregeln, Sicherheitseinstellungen usw.

Diese Datei enthält KEINE gerätespezifischen Informationen, einschließlich:

- Gerätename
- Netzwerkeinstellungen (IP-Adresse, Gateway, Netzmaske usw.)
- Geräteprotokolle
- Umgebungssensornamen
- Umgebungssensor-Status und -Werte
- SSL-Zertifikat
- Namen von Asset-Management-Sensoren und Rackeinheiten
- SNMP-Name, Standort und Kontakt
- Serverüberwachungseinträge

Da die Datums- und Uhrzeiteinstellungen in der Konfigurationsdatei gespeichert werden, sollten Benutzer vorsichtig sein, wenn sie die Konfigurationsdatei an die EMX-Geräte in einer anderen Zeitzone als der des Quellgeräts verteilen.

So speichern Sie eine Konfigurationsdatei:

1. Wählen Sie "Maintenance" > "Bulk Configuration" (Wartung > Sammelkonfiguration) aus. Das Dialogfeld "Bulk Configuration" (Sammelkonfiguration) wird angezeigt.
2. Klicken Sie auf "Download Bulk Configuration" (Sammelkonfiguration herunterladen).
3. Wenn Sie vom Webbrowser aufgefordert werden, die Konfigurationsdatei zu öffnen oder zu speichern, klicken Sie auf "Save" (Speichern). Wählen Sie den gewünschten Speicherort aus und speichern Sie die Konfigurationsdatei auf dem PC.

Die Datei wird im XML-Format gespeichert, und ihr Inhalt wird mit dem AES-128-Verschlüsselungsalgorithmus verschlüsselt.

Kopieren einer EMX-Konfiguration

Ein Zielgerät ist ein EMX-Gerät, auf dem die Konfigurationsdatei eines anderen EMX-Geräts geladen wird.

Durch das Kopieren einer EMX-Konfiguration auf ein Zielgerät werden die Einstellungen dieses EMX-Geräts angepasst, sodass sie mit denen des EMX-Quellgeräts übereinstimmen. Um eine EMX-Konfiguration erfolgreich zu kopieren, muss Folgendes beachtet werden:

- Bei dem Benutzer muss es sich um den Administrator handeln. Oder die Administratorrolle wird dem Benutzer zugewiesen.
- Das EMX-Zielgerät muss dem Modelltyp des EMX-Quellgeräts entsprechen.
- Das EMX-Zielgerät muss dieselbe Firmwareversion aufweisen wie das EMX-Quellgerät.

So kopieren Sie eine EMX-Konfiguration:

1. Melden Sie sich auf der Webschnittstelle des Zielgeräts an.
2. Wenn die Firmwareversion des Zielgeräts nicht mit der des Quellgeräts übereinstimmt, aktualisieren Sie die Firmware des Zielgeräts. Siehe ***Firmware-Upgrade*** (auf Seite 96).
3. Wählen Sie "Maintenance" > "Bulk Configuration" (Wartung > Sammelkonfiguration) aus. Das Dialogfeld "Bulk Configuration" (Sammelkonfiguration) wird angezeigt.
4. Klicken Sie im Bereich "Copy Bulk Configuration" (Sammelkonfiguration kopieren) auf "Browse" (Durchsuchen), und wählen Sie die auf dem PC gespeicherte Konfigurationsdatei aus.
5. Klicken Sie auf "Upload & Restore Bulk Configuration" (Sammelkonfiguration hochladen & wiederherstellen), um die Datei zu kopieren.
6. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
7. Warten Sie, bis das EMX-Gerät zurückgesetzt wurde und die Seite "Login" (Anmelden) wieder angezeigt wird. Diese zeigt an, dass das Kopieren der Konfiguration abgeschlossen ist.

Firmware-Upgrade

Sie können das EMX-Gerät aktualisieren, um die neuesten Erweiterungen, Verbesserungen und Funktionen nutzen zu können

Die Firmware-Dateien von EMX können von der Raritan-Website im ***Bereich "Firmware und Dokumentation"*** (***http://www.raritan.com/support/firmware-and-documentation/***) heruntergeladen werden.

Aktualisieren der Firmware

Um die Firmware des EMX-Geräts zu aktualisieren, müssen Sie sich als Systemadministrator oder als Benutzer mit der Berechtigung zur Firmware-Aktualisierung anmelden.

Falls für Ihr Modell zutreffend, laden Sie die neueste Firmware-Datei von der Raritan-Website herunter, lesen Sie die Versionshinweise und starten Sie anschließend die Aktualisierung. Wenn Sie Fragen oder Bedenken zur Aktualisierung haben, wenden Sie sich VOR der Aktualisierung an den technischen Kundendienst von Raritan.

Warnung: Führen Sie die Firmware-Aktualisierung NICHT über eine Drahtlosverbindung aus.

So aktualisieren Sie die Firmware:

1. Wählen Sie "Maintenance" > "Update Firmware" (Wartung > Firmware aktualisieren) aus. Das Dialogfeld "Firmware Update" (Firmware aktualisieren) wird eingeblendet.
2. Klicken Sie im Feld "Firmware File" (Firmware-Datei) auf "Browse" (Durchsuchen), um die entsprechende Firmware-Datei auszuwählen.
3. Klicken Sie auf "Upload" (Hochladen). Der Status für das Hochladen wird in der Statusleiste angezeigt.
4. Nachdem das Hochladen abgeschlossen ist, werden die Versionsinformationen zur vorhandenen und hochgeladenen Firmware angezeigt, damit Sie die Aktualisierung endlich abschließen können.
5. Um das Zertifikat der hochgeladenen Firmware anzuzeigen, klicken Sie auf "View Certificate" (Zertifikat anzeigen). **(Optional)**
6. Um mit der Aktualisierung fortzufahren, klicken Sie auf "Update Firmware" (Firmware aktualisieren). Die Aktualisierung kann mehrere Minuten dauern.

   Warnung: Schalten Sie das EMX-Gerät während der Aktualisierung NICHT aus.

   Während der Firmware-Aktualisierung:

   - In der Webschnittstelle wird eine Statusleiste angezeigt, die den Aktualisierungsstatus wiedergibt.
   - Es können sich keine Benutzer bei der EMX-Einheit anmelden.
   - In der Webschnittstelle wird allen angemeldeten Benutzern die Zeitüberschreitungsmeldung von EMX angezeigt, und in der Statusleiste wird "disconnected" (getrennt) angezeigt.
   - Ein eventueller Benutzerverwaltungsvorgang wird ausgesetzt.

7. Nachdem die Aktualisierung abgeschlossen ist, wird eine Meldung mit dem Hinweis angezeigt, dass die Aktualisierung erfolgreich war.
8. Das EMX-Gerät wird zurückgesetzt, und die Anmeldeseite wird erneut eingeblendet. Sie können sich nun wieder anmelden und mit Ihrem Vorgang fortfahren.

Hinweis 1: Die anderen angemeldeten Benutzer werden ebenfalls abgemeldet, wenn die Firmware-Aktualisierung abgeschlossen ist.

Hinweis 2: Wenn Sie die EMX-Einheit zusammen mit einem SNMP-Manager verwenden, sollten Sie die >ProductName<-MIB nach der Aktualisierung der Firmware erneut herunterladen. Damit wird sichergestellt, dass für den SNMP-Manager die neueste MIB zur Verfügung steht. Siehe **Verwenden von SNMP** *(auf Seite 217).*

Anzeigen des Protokolls zur Firmwareaktualisierung

Das Protokoll zum Firmware-Upgrade ist, sofern verfügbar, permanent auf dem EMX-Gerät gespeichert.

Dieses Protokoll gibt den Zeitpunkt des Firmware-Upgrades, die vorherige und die neue Version, die mit dem Firmware-Upgrade verbunden ist, und das Upgrade-Ergebnis an.

So zeigen Sie das Protokoll zur Firmwareaktualisierung an:

1. Wählen Sie "Maintenance > View Firmware Update History" (Wartung > Protokoll zur Firmwareaktualisierung anzeigen). Das Dialogfeld "Firmware Update History" (Protokoll zur Firmwareaktualisierung) wird angezeigt.
   - Datum und Uhrzeit des Firmware-Upgrades
   - Vorherige Firmwareversion
   - Version der aktualisierten Firmware
   - Ergebnis des Firmware-Upgrades
2. Sie können die Anzahl der angezeigten Spalten ändern oder die Reihenfolge der Liste neu sortieren, um die Daten lesefreundlich darzustellen. Siehe Ändern der Listenansicht.
3. Um die Details eines Firmware-Upgrades anzuzeigen, wählen Sie das Ereignis aus und klicken Sie auf "Details" oder doppelklicken Sie einfach auf das Ereignis. Das Dialogfeld "Firmware Update Details" (Details zur Firmwareaktualisierung) wird angezeigt, das ausführliche Informationen über das ausgewählte Ereignis enthält.
4. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Vollständige Notfallwiederherstellung

Schlägt das Firmware-Upgrade fehl, sodass das EMX-Gerät nicht mehr funktioniert, können Sie es mit einem speziellen Dienstprogramm wiederherstellen, anstatt es an Raritan zu senden.

Kontaktieren Sie den technischen Support von Raritan, um das Wiederherstellungsdienstprogramm zu erhalten. Dieses kann unter Windows XP/Vista/7 und Linux eingesetzt werden. Für den Wiederherstellungsprozess benötigen Sie außerdem die passende EMX-Firmware-Datei.

Aktualisieren der Assetsensor-Firmware

Nachdem der Assetsensor an das EMX-Gerät angeschlossen wurde, vergleicht er automatisch seine eigene Firmwareversion mit der Version der Assetsensor-Firmware, die in der EMX-Firmware gespeichert ist. Sind die beiden Versionen verschieden, lädt der Assetsensor die neue Firmware automatisch vom EMX-Gerät herunter, um seine eigene Firmware zu aktualisieren.

Während der Firmwareaktualisierung geschieht Folgendes:

- Die LEDs des Assetsensors leuchten, wobei die Farbe der blinkenden LEDs von rot nach grün wechselt.
- Firmware-Upgrades werden in der EMX-Webschnittstelle angezeigt.
- Ein SNMP-Trap wird gesendet, um auf das Firmware-Upgrade hinzuweisen.

Netzwerkdiagnose

Die EMX-Einheit bietet auf der Webschnittstelle die folgenden Werkzeuge zur Diagnose potenzieller Probleme mit dem Netzwerk.

- Ping
- Trace Route
- List TCP Connections

Tipp: Diese Netzwerkdiagnosetools sind auch über die CLI verfügbar. Siehe **Behebung von Netzwerkproblemen** *(auf Seite 333).*

Überprüfen eines Hosts mit dem Ping-Tool

Mit dem Ping-Tool können Sie prüfen, ob ein Host über das Netzwerk oder das Internet erreichbar ist.

So führen Sie das Ping-Tool für einen Host aus:

1. Wählen Sie "Maintenance > Network Diagnostics > Ping" (Wartung > Netzwerkdiagnose > Ping). Das Dialogfeld "Ping Network Host" (Netzwerkhost mit Ping überprüfen) wird angezeigt.
2. Geben Sie im Feld "Host Name" (Hostname) den Namen oder die IP-Adresse des Hosts ein, den Sie überprüfen möchten.
3. Geben Sie im Feld "Number of Requests" (Anzahl Anfragen) einen Wert bis 10 ein, oder passen Sie den Wert durch klicken auf einen der Pfeile an. Dieser Wert legt fest, wie viele Pakete gesendet werden, um den Host mit Ping zu überprüfen.
4. Klicken Sie auf "Run Ping" (Ping ausführen), um den Host mit Ping zu überprüfen. Ein Dialogfeld mit den Ping-Ergebnissen wird angezeigt.
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Verfolgen der Netzwerkroute

Mit "Trace Route" (Route verfolgen) können Sie die Route über das Netzwerk zwischen zwei Hosts oder Systemen ermitteln.

So verfolgen Sie die Route für einen Host:

1. Wählen Sie "Maintenance > Network Diagnostics > Trace Route" (Wartung > Netzwerkdiagnose > Route verfolgen). Das Dialogfeld "Trace Route to Host" (Route zum Host verfolgen) wird angezeigt.
2. Geben Sie die IP-Adresse oder den Namen des Hosts, dessen Route Sie überprüfen möchten, in das Feld "Host Name" (Hostname) ein.
3. Klicken Sie auf "Run" (Ausführen). Ein Dialogfeld mit den Ergebnissen der Routenverfolgung wird angezeigt.
4. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Auflisten von TCP-Verbindungen

Sie können mit "List TCP Connections" (TCP-Verbindungen auflisten) eine Liste der TCP-Verbindungen anzeigen.

So verfolgen Sie die Route für einen Host:

1. Wählen Sie "Maintenance > Network Diagnostics > List TCP Connections" (Wartung > Netzwerkdiagnose > TCP-Verbindungen auflisten). Das Dialogfeld für TCP-Verbindungen wird angezeigt.
2. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Herunterladen von Diagnoseinformationen

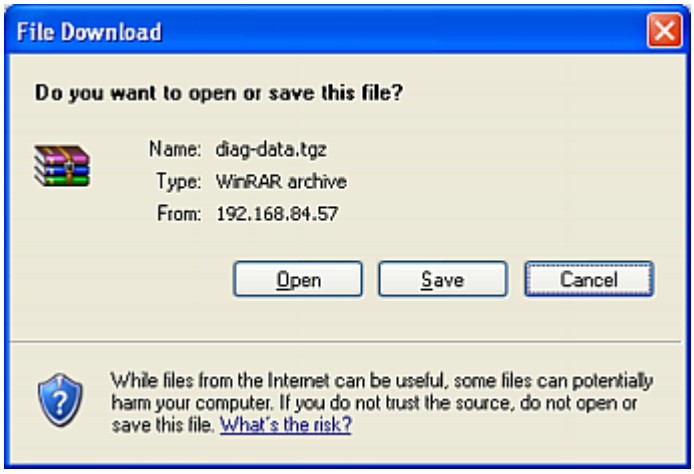
Wichtig: Diese Funktion wird von Raritan-Technikern im Außendienst oder von Ihnen verwendet, nachdem Sie der technische Kundendienst von Raritan dazu angewiesen hat.

Sie können die Diagnosedatei vom EMX-Gerät auf einen Client-Rechner herunterladen. Die Datei ist als .tgz-Datei komprimiert und muss zur Auswertung an den technischen Kundendienst von Raritan gesendet werden.

Diese Funktion ist nur für Benutzer mit Administratorberechtigungen zugänglich.

So rufen Sie eine Diagnosedatei ab:

1. Wählen Sie "Maintenance > Download Diagnostic Information" (Wartung > Diagnoseinformationen herunterladen). Das Dialogfeld "File Download" (Datei-Download) wird angezeigt.


File Download
Do you want to open or save this file?
Name: diag-data.tgz
Type: WinRAR archive
From: 192.168.84.57
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

2. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.

3. Wechseln Sie zum gewünschten Verzeichnis, und klicken Sie auf "Save" (Speichern).
4. Senden Sie die Datei entsprechend den Anweisungen des technischen Kundendiensts von Raritan per E-Mail.

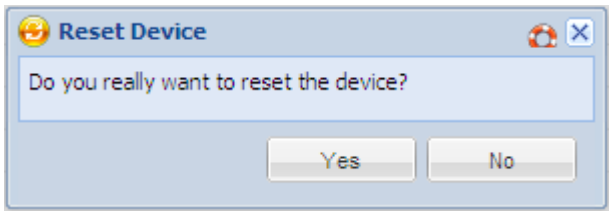
Neustart des EMX-Geräts

Sie können das EMX-Gerät über die Webschnittstelle extern neu starten. Anders als beim Wiederherstellen der Werkseinstellungen wird die Konfiguration des Geräts bei einem Neustart der EMX-Einheit nicht zurückgesetzt.

Hinweis: Beim Neustart der EMX-Einheit werden die per Webcam aufgenommenen Momentaufnahmen gelöscht.

So starten Sie das Gerät neu:

1. Wählen Sie "Maintenance" > "Unit Reset" (Wartung > Einheit zurücksetzen) aus. Das Dialogfeld "Reset Device" (Gerät zurücksetzen) wird eingeblendet.



2. Klicken Sie auf "Yes" (Ja), um die EMX-Einheit zurückzusetzen.
3. Es wird eine Meldung mit einem Countdown-Timer angezeigt, der die verbleibende Zeit des Vorgangs anzeigt. Der Vorgang dauert etwa eine Minute.
4. Nachdem das Zurücksetzen abgeschlossen ist, wird die Anmeldeseite geöffnet. Sie können sich nun wieder bei dem EMX-Gerät anmelden.

Hinweis: Falls nach dem Zurücksetzen nicht die Anmeldeseite angezeigt wird, klicken Sie in der Meldung auf den unterstrichenen Text "this link" (Dieser Link).

Wiederherstellen der werksseitigen Standardeinstellungen

Aus Sicherheitsgründen kann das EMX-Gerät nur an der lokalen Konsole auf die werkseitigen Standardeinstellungen zurückgesetzt werden.

Wichtig: Bevor Sie die EMX-Einheit auf die werkseitigen Standardeinstellungen zurücksetzen, sollten Sie sich vor Augen führen, dass dadurch vorhandene Daten und angepasste Einstellungen gelöscht werden, wie z. B. Benutzerprofile, Schwellenwerte usw.

Zum Zurücksetzen der EMX-Einheit können Sie entweder die Reset-Taste oder die Befehlszeilenschnittstelle (CLI) verwenden.

So setzen Sie das Gerät mit der Reset-Taste auf die werkseitigen Einstellungen zurück:

1. Schließen Sie einen Computer an das EMX-Gerät an. Siehe ***Anschließen der EMX-Einheit an einen Computer*** (auf Seite 11).
2. Öffnen Sie in EMX über ein Terminalemulationsprogramm, wie HyperTerminal, Kermit oder PuTTY, ein Terminalfenster.
3. Drücken Sie mehrmals hintereinander die Esc-Taste auf der Tastatur, während Sie gleichzeitig die Reset-Taste am EMX-Gerät drücken (und wieder loslassen). Nach ca. einer Sekunde sollte eine Eingabeaufforderung (=>) angezeigt werden.
4. Geben Sie *defaults* (Standardeinstellungen) ein, um <ProductName > auf die werkseitigen Standardeinstellungen zurückzusetzen.
5. Warten Sie, bis die Eingabeaufforderung "Username" (Benutzername) angezeigt wird, die darauf hinweist, dass das Zurücksetzen abgeschlossen ist.

Hinweis: Auf älteren Windows-Systemen vor Windows Vista ist HyperTerminal vorhanden. Bei Windows Vista oder neueren Versionen können Sie PuTTY verwenden, ein kostenloses Programm, das aus dem Internet geladen werden kann. Einzelheiten zur Konfiguration von PuTTY finden Sie in der Dokumentation des Programms.

Kapitel 6 Security (Sicherheit)

In diesem Kapitel

Zugriffssteuerung.....104
Einrichten eines SSL-Zertifikats 122
Einrichten der LDAP-Authentifizierung.....129

Zugriffssteuerung

Die EMX-Einheit bietet Werkzeuge, mit denen der Zugriff gesteuert werden kann. Sie können die HTTPS-Verschlüsselung erzwingen, die interne Firewall aktivieren, Firewall-Regeln erstellen und Anmeldebeschränkungen festlegen.

Tipp: Sie können das Zertifikat auch erstellen und installieren oder externe Authentifizierungsserver für die Zugriffssteuerung einrichten. Siehe **Einrichten eines SSL-Zertifikats** *(auf Seite 122) und* **Einrichten der LDAP-Authentifizierung** *(auf Seite 129).*

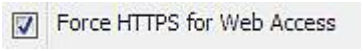
Erzwingen der HTTPS-Verschlüsselung

HTTPS verwendet zum Verschlüsseln des gesamten Verkehrs an das und vom EMX-Gerät die SSL-Technologie (Secure Sockets Layer) und ist somit ein sichereres Protokoll als HTTP.

Sie können erzwingen, dass Benutzer die EMX-Schnittstelle nur über das HTTPS-Protokoll aufrufen können. Dieses Protokoll ist standardmäßig aktiviert.

So erzwingen Sie den HTTPS-Zugriff auf die Webschnittstelle:

1. Wählen Sie "Device Settings" > "Security" > "Force HTTPS for Web Access" (Geräteeinstellungen > Sicherheit > HTTPS für Webzugriff erzwingen) aus.
2. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie auf "Yes" (Ja), um den HTTP-Dienst zu erzwingen.
3. Wählen Sie "Device Settings" > "Security" (Geräteeinstellungen > Sicherheit) aus, um zu überprüfen, ob das Kontrollkästchen "Force HTTPS for Web Access" (HTTPS für Webzugriff erzwingen) aktiviert ist (siehe Abbildung).



Wenn das Kontrollkästchen nicht aktiviert ist, wiederholen Sie diese Schritte.

Nachdem Sie das HTTPS-Protokoll aktiviert haben, werden alle Zugriffversuche über HTTP automatisch an HTTPS umgeleitet.

Konfigurieren der Firewall

Die <ProdcutName>-Einheit verfügt über eine Firewall, mit der verhindert werden kann, dass bestimmte IP-Adressen und IP-Adressbereiche auf das EMX-Gerät zugreifen. Standardmäßig ist die Firewall deaktiviert.

So konfigurieren Sie die Firewall:

1. Aktivieren Sie die Firewall. Siehe ***Aktivieren der Firewall*** (auf Seite 105).
2. Legen Sie die Standardrichtlinie fest. Siehe ***Ändern der Standardrichtlinie*** (auf Seite 106).
3. Erstellen Sie Firewall-Regeln, um anzugeben, welche Adressen zugelassen oder abgelehnt werden. Siehe ***Erstellen von Firewall-Regeln*** (auf Seite 107).

Änderungen an den Firewall-Regeln werden unverzüglich wirksam. Alle nicht autorisierten IP-Aktivitäten werden sofort beendet.

Hinweis: Mit der standardmäßigen Deaktivierung der Firewall soll verhindert werden, dass Benutzer ihren Zugriff auf das Gerät versehentlich selbst sperren.

Aktivieren der Firewall

Die Firewall-Regeln werden erst wirksam, nachdem die Firewall aktiviert wurde.

So aktivieren Sie die EMX-Firewall:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.
2. Um die IPv4-Firewall zu aktivieren, klicken Sie auf die Registerkarte "IPv4", und aktivieren Sie das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren).
3. Um die IPv6-Firewall zu aktivieren, klicken Sie auf die Registerkarte "IPv6", und aktivieren Sie das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren).
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern der Standardrichtlinie

Nachdem Sie die Firewall aktiviert haben, wird der Verkehr gemäß der Standardrichtlinie von allen IP-Adressen zugelassen. Das bedeutet, dass nur IP-Adressen, die von einer bestimmten Regel abgelehnt werden, KEINEN Zugriff auf die EMX-Einheit haben.

Sie können die Standardrichtlinie in "Drop" (Trennen) oder "Reject" (Ablehnen) ändern. In diesem Fall wird der Verkehr von allen IP-Adressen verworfen, es sei denn, die IP-Adressen werden durch eine bestimmte Regel zugelassen.

So ändern Sie die Standardrichtlinie:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.
2. So legen Sie die Standardrichtlinie für IPv4-Adressen fest:
   a. Klicken Sie ggf. auf die Registerkarte "IPv4".
   b. Stellen Sie sicher, dass das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren) aktiviert ist.
   c. Die Standardrichtlinie wird im Feld "Default Policy" (Standardrichtlinie) angezeigt. Wählen Sie zum Ändern eine andere Richtlinie aus der Dropdown-Liste aus.
      - Accept (Zulassen): Lässt Verkehr von allen IPv4-Adressen zu.
      - Drop (Trennen): Verwirft den Verkehr von allen IPv4-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
      - Reject (Ablehnen): Verwirft den Verkehr von allen IPv4-Adressen, und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.
3. So legen Sie die Standardrichtlinie für IPv6-Adressen fest:
   a. Klicken Sie auf die Registerkarte "IPv6".
   b. Stellen Sie sicher, dass das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren) aktiviert ist.
   c. Die Standardrichtlinie wird im Feld "Default Policy" (Standardrichtlinie) angezeigt. Wählen Sie zum Ändern eine andere Richtlinie aus der Dropdown-Liste aus.

- Accept (Zulassen): Lässt Verkehr von allen IPv6-Adressen zu.
- Drop (Trennen): Verwirft den Verkehr von allen IPv6-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
- Reject (Ablehnen): Verwirft den Verkehr von allen IPv6-Adressen, und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.

4. Klicken Sie auf "OK", um die Änderungen zu speichern. Die neue Standardrichtlinie wird angewendet.

Erstellen von Firewall-Regeln

Mit Firewall-Regeln wird der Verkehr zum EMX-Gerät auf der Grundlage der IP-Adresse des sendenden Hosts zugelassen oder abgelehnt. Beachten Sie bei der Erstellung von Firewall-Regeln Folgendes:

- **Die Reihenfolge der Regeln ist wichtig.**

  Wenn der Verkehr das EMX-Gerät erreicht, werden die Regeln in numerischer Reihenfolge ausgeführt. Nur die erste Regel, die mit der IP-Adresse übereinstimmt, bestimmt, ob der Verkehr zugelassen oder abgelehnt wird. Alle nachfolgenden Regeln, die mit der IP-Adresse übereinstimmen, werden von der EMX-Einheit ignoriert.

- **Eine Subnetzmaske kann erforderlich sein.**

  Bei der Eingabe der IP-Adresse müssen Sie eventuell SOWOHL die Adresse ALS AUCH eine Subnetzmaske angeben. Die Standard-Subnetzmaske ist /32 (d.h. 255.255.255.255). Sie müssen nur eine Subnetzmaske angeben, wenn diese sich vom Standard unterscheidet. Verwenden Sie z. B. folgendes Format, um eine einzelne Adresse in einem Netzwerk der Netzwerkklasse C anzugeben:

  x.x.x.x/24

  Dabei steht */24* für die Subnetzmaske 255.255.255.0.

  Um ein vollständiges Subnetz oder einen Adressbereich anzugeben, ändern Sie die Subnetzmaske entsprechend.

Hinweis: Der gültige IP-Adressbereich liegt zwischen 0.0.0.0 und 255.255.255.255. Die IP-Adressen müssen innerhalb dieses Bereichs liegen.

So erstellen Sie Firewall-Regeln:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.

2. Klicken Sie auf die Registerkarte "IPv4" zum Erstellen von Firewall-Regeln, oder klicken Sie auf die Registerkarte "IPv6" zum Erstellen von IPv6-Firewall-Regeln.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Erstellen Sie die Regeln In der Tabelle finden Sie weitere Operationen.

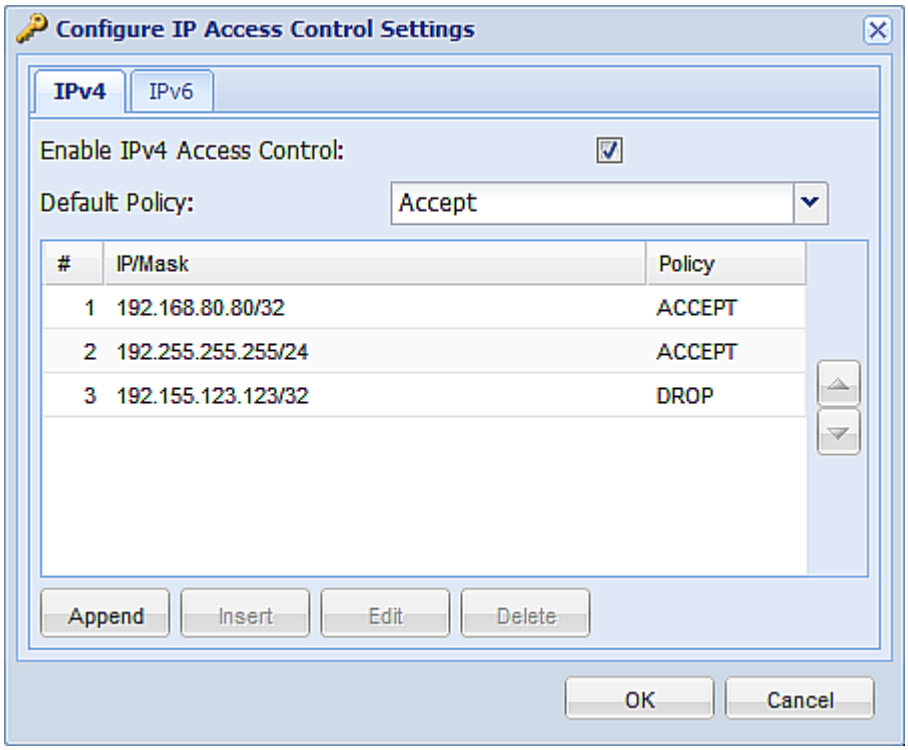
Aktion	Vorgehensweise

Eine Regel am Ende der Regelliste anfügen	▪ Klicken Sie auf "Append" (Anfügen). Das Dialogfeld "Append new Rule" (Neue Regel anhängen) wird angezeigt.
	▪ Geben Sie im Feld "IP/Mask" (IP/Maske) eine IP-Adresse und Subnetzmaske ein.
	▪ Wählen Sie in der Dropdown-Liste im Feld "Policy" (Richtlinie) entweder "Accept" (Zulassen), "Drop" (Trennen) oder "Reject" (Ablehnen) aus.
	  ▪ Accept (Zulassen): Lässt Verkehr von den angegebenen IP-Adressen zu.
	  ▪ Drop (Trennen): Verwirft den Verkehr von den angegebenen IP-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
	  ▪ Reject (Ablehnen): Verwirft den Verkehr von den angegebenen IP-Adressen und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.
	▪ Klicken Sie auf "OK", um die Änderungen zu speichern.
	Der Regel wird automatisch vom System eine Nummer zugewiesen.

Aktion	Vorgehensweise

Eine Regel zwischen zwei vorhandenen Regeln einfügen	▪ Wählen Sie die Regel aus, über der Sie eine neue Regel einfügen möchten. Wenn Sie z. B. zwischen den Regeln 3 und 4 eine Regel einfügen möchten, wählen Sie 4 aus.
	▪ Klicken Sie auf "Insert" (Einfügen). Das Dialogfeld "Insert new Rule" (Neue Regel einfügen) wird angezeigt.
	▪ Geben Sie im Feld "IP/Mask" (IP/Maske) eine IP-Adresse und Subnetzmaske ein.
	▪ Wählen Sie in der Dropdown-Liste im Feld "Policy" (Richtlinie) entweder "Accept" (Zulassen), "Drop" (Trennen) oder "Reject" (Ablehnen) aus.
	  ▪ Accept (Zulassen): Lässt Verkehr von den angegebenen IP-Adressen zu.
	  ▪ Drop (Trennen): Verwirft den Verkehr von den angegebenen IP-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
	  ▪ Reject (Ablehnen): Verwirft den Verkehr von den angegebenen IP-Adressen und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.
	▪ Klicken Sie auf "OK", um die Änderungen zu speichern.
	Das System fügt die Regel ein und nummeriert die folgenden Regeln automatisch neu.

5. Wenn Sie fertig sind, werden die Regeln im Dialogfeld "Configure IP Access Control Settings" (Einstellungen für IP-Zugriffssteuerung konfigurieren) angezeigt.



6. Klicken Sie auf "OK", um die Änderungen zu speichern. Die Regeln werden angewendet.

Bearbeiten von Firewall-Regeln

Wenn für eine bestehende Firewall-Regel Aktualisierungen des IP-Adressbereichs und/oder der Richtlinie erforderlich sind, nehmen Sie entsprechende Änderungen vor.

So ändern Sie eine Firewall-Regel:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu ändern. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu ändern.

3. Achten Sie darauf, dass das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Wählen Sie die zu ändernde Regel in der Regelliste aus.
5. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf die Regel. Das Dialogfeld "Edit Rule" (Regel bearbeiten) wird eingeblendet.
6. Nehmen Sie an den angezeigten Informationen die Änderungen vor.
7. Klicken Sie auf "OK", um die Änderungen zu speichern.
8. Klicken Sie auf "OK", um das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) zu verlassen, ansonsten gehen die Änderungen verloren.

Sortieren von Firewall-Regeln

Die Regelreihenfolge bestimmt, welche Regel, die mit IP-Adresse übereinstimmt, ausgeführt wird.

So sortieren Sie Firewall-Regeln:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu sortieren. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu sortieren.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Klicken Sie auf eine bestimmte Regel, um sie auszuwählen.
5. Klicken Sie auf oder , um die ausgewählte Regel nach oben oder unten zu verschieben, bis sie die gewünschte Position in der Reihenfolge erreicht hat.
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen von Firewall-Regeln

Wenn eine Firewall-Regel veraltet oder unnötig wird, entfernen Sie sie aus der Regelliste.

So löschen Sie eine gruppenbasierte Zugriffssteuerungsregel:

1. Wählen Sie "Device Settings" > "Security" > "IP Access Control" (Geräteeinstellungen > Sicherheit > IP-Zugriffssteuerung) aus. Das Dialogfeld "Configure IP Access Control Settings" (Einstellungen für die IP-Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu löschen. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu löschen.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable IPv4 Access Control" (IPv4-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable IPv6 Access Control" (IPv6-Zugriffssteuerung aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Wählen Sie die Regel aus, die Sie löschen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
5. Klicken Sie auf "Delete" (Löschen).
6. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie auf "Yes" (Ja), um die ausgewählte(n) Regel(n) aus der Regelliste zu löschen.
7. Klicken Sie auf "OK", um die Änderungen zu speichern.

Einrichten von Benutzeranmeldesteuerungen

Um den unbefugten Zugriff auf die EMX-Einheit und die daran angeschlossenen Geräte zu erschweren, können Anmeldesteuerungen eingerichtet werden. Sie können festlegen, dass Benutzer nach einer bestimmten Anzahl von Anmeldefehlversuchen gesperrt werden, die Anzahl der Benutzer beschränken, die sich gleichzeitig mit demselben Anmeldenamen anmelden können, und bestimmen, dass Benutzer sichere Kennwörter erstellen müssen.

Aktivieren der Benutzersperrung

Mit der Benutzersperrung wird festgelegt, wie viele Anmeldefehlversuche bei der EMX-Einheit ein Benutzer hat, bis er gesperrt wird.

Beachten Sie, dass diese Funktion nur für die lokale Authentifizierung gilt und nicht für die Authentifizierung über externe AA-Server.

Hinweis: Wenn eine Benutzersperrung auftritt, können Sie diesen Benutzer entsperren, indem Sie den CLI-Befehl "unblock" (entsperren) über eine serielle Verbindung verwenden. Siehe **Entsperren eines Benutzers** *(siehe "***Aufheben der Sperrung eines Benutzers***" auf Seite 331).*

So aktivieren Sie die Benutzersperrung:

1. Wählen Sie "Device Settings" > "Security" > "Login Settings" (Geräteeinstellungen > Sicherheit > Anmeldeeinstellungen) aus. Das Dialogfeld "Login Settings" (Anmeldeeinstellungen) wird angezeigt.
2. Suchen Sie den Abschnitt "User Blocking" (Benutzersperrung).
3. Um die Funktion der Benutzersperrung zu aktivieren, markieren Sie das Kontrollkästchen "Block user on login failure" (Benutzer bei Fehlanmeldung sperren).
4. Geben Sie im Feld "Maximum number of failed logins" (Max. Anzahl der Anmeldefehlversuche) einen Wert ein. Dabei handelt es sich um die maximale Anzahl der Anmeldefehlversuche, die der Benutzer zur Verfügung hat, bis er für den Zugriff auf das EMX-Gerät gesperrt wird.
5. Um festzulegen, wie lange die Anmeldung gesperrt ist, wählen Sie die gewünschte Zeitdauer aus der Dropdown-Liste im Feld "Block timeout" (Sperrdauer) aus. Im Folgenden werden die verfügbaren Optionen beschrieben.
   - Infinite (Unbegrenzt): Diese Option legt keine Zeitbegrenzung für die Sperrung der Anmeldung fest.
   - X min: Diese Option legt die Zeitbegrenzung auf X Minuten fest, wobei X eine Zahl ist.
   - X h: Diese Option legt die Zeitbegrenzung auf X Stunden fest, wobei X eine Zahl ist.
   - 1 d: Diese Option legt die Zeitbegrenzung auf 1 Tag fest.

   Tipp: Wenn die gewünschte Zeitoption nicht aufgeführt ist, können Sie die gewünschte Zeit in das Feld eingeben. Sie können beispielsweise "4 min" eingeben, um die Zeit auf 4 Minuten einzustellen.

   ---
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Aktivieren von Anmeldebeschränkungen

Mit Anmeldebeschränkungen können Sie festlegen, ob ein Anmeldename von mehreren Benutzern gleichzeitig verwendet werden kann und wie lange Benutzer inaktiv sein dürfen, bis sie aufgefordert werden, sich abzumelden.

So aktivieren Sie Anmeldebeschränkungen:

1. Wählen Sie "Device Settings" > "Security" > "Login Settings" (Geräteeinstellungen > Sicherheit > Anmeldeeinstellungen) aus. Das Dialogfeld "Login Settings" (Anmeldeeinstellungen) wird angezeigt.
2. Suchen Sie den Abschnitt "Login Limitations" (Anmeldebeschränkungen).
3. Um zu verhindern, dass ein Anmeldename von mehreren Benutzern gleichzeitig verwendet werden kann, aktivieren Sie das Kontrollkästchen "Prevent concurrent login with same username" (Gleichzeitige Anmeldung mit dem selben Benutzernamen verhindern).
4. Wählen Sie eine Zeitoption im Feld "Idle Timeout" (Zeitlimit für Inaktivität) aus, um festzulegen, wie lange ein Benutzer inaktiv sein darf, bevor die aktive Sitzung von der EMX-Einheit beendet wird. Der Standardwert lautet 10 Minuten.
   - X min: Diese Option legt die Zeitbegrenzung auf X Minuten fest, wobei X eine Zahl ist.
   - X h: Diese Option legt die Zeitbegrenzung auf X Stunden fest, wobei X eine Zahl ist.
   - 1 d: Diese Option legt die Zeitbegrenzung auf 1 Tag fest.

   Tipp: Wenn die gewünschte Zeitoption nicht aufgeführt ist, können Sie die gewünschte Zeit in das Feld eingeben. Sie können beispielsweise "4 min" eingeben, um die Zeit auf 4 Minuten einzustellen.
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Tipp: Das Zeitlimit für die Inaktivität sollte, wenn möglich, bei 20 Minuten oder weniger belassen werden. Dadurch wird die Anzahl an inaktiven aber verbundenen Sitzungen sowie die Anzahl gleichzeitig eingegebener Befehle an die EMX-Einheit reduziert.

Aktivieren von sicheren Kennwörtern

Durch die Verwendung sicherer Kennwörter wird Angreifern der Zugriff auf das EMX-Gerät erschwert, da die Kennwörter nur schwer zu erraten sind. Standardmäßig sollten sichere Kennwörter aus mindestens acht Zeichen bestehen und Klein- und Großbuchstaben, Ziffern sowie Sonderzeichen (wie z. B. @ oder &) enthalten.

So legen Sie fest, dass Benutzer sichere Kennwörter erstellen müssen:

1. Wählen Sie "Device Settings" > "Security" > "Password Policy" (Geräteeinstellungen > Sicherheit > Kennwortrichtlinie) aus. Das Dialogfeld "Password Policy" (Kennwortrichtlinie) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Strong Passwords" (Sichere Kennwörter). Die Standardeinstellungen lauten wie folgt:

Minimum length of strong password (Mindestlänge des sicheren Kennworts)	= 8 Zeichen
Maximum length of strong password (Höchstlänge des sicheren Kennworts)	= 32 Zeichen
Enforce at least one lower case character (Mindestens einen Kleinbuchstaben erzwingen)	= Aktiviert
Enforce at least one upper case character (Mindestens einen Großbuchstaben erzwingen)	= Aktiviert
Enforce at least one numeric character (Mindestens eine Ziffer erzwingen)	= Aktiviert
At least one special character (Mindestens ein Sonderzeichen)	= Aktiviert
Number of restricted passwords in history (Anzahl unzulässiger Kennwörter im Verlauf)	= 5

Hinweis: Die maximal zulässige Kennwortlänge für die EMX-Einheit ist 32 Zeichen.

3. Ändern Sie die Standardeinstellungen nach Bedarf.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Aktivieren der Kennworterneuerung

Über die Kennworterneuerung wird festgelegt, ob Benutzer ihr Kennwort in regelmäßigen Abständen ändern müssen. Das Standardintervall ist 60 Tage.

So legen Sie fest, dass Benutzer Kennwörter regelmäßig ändern müssen:

1. Wählen Sie "Device Settings" > "Security" > "Password Policy" (Geräteeinstellungen > Sicherheit > Kennwortrichtlinie) aus. Das Dialogfeld "Password Policy" (Kennwortrichtlinie) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Password Aging" (Kennworterneuerung), um die Funktion der Kennworterneuerung zu aktivieren.
3. Um festzulegen, wie oft Benutzer aufgefordert werden, ihre Kennwörter zu ändern, wählen Sie eine Anzahl von Tagen im Feld "Password Aging Interval" (Intervall der Kennworterneuerung) aus. Nach Ablauf dieser Anzahl von Tagen müssen Benutzer ihre Kennwörter ändern.

   Tipp: Wenn die gewünschte Zeitoption nicht aufgeführt ist, können Sie die gewünschte Zeit in das Feld eingeben. Sie können z. B. "9 d" eingeben, um den Zeitraum für die Kennworterneuerung auf 9 Tage festzulegen.

4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Einrichten von benutzerfunktionsbasierten Zugriffssteuerungsregeln

Benutzerfunktionsbasierte Zugriffssteuerungsregeln sind mit Firewall-Regeln vergleichbar. Erstere werden jedoch auf Mitglieder, die eine bestimmte Benutzerfunktion gemeinsam haben, angewendet. Damit können Sie einer bestimmten Benutzerfunktion Systemberechtigungen auf der Grundlage der IP-Adressen zuweisen.

So richten Sie benutzerfunktionsbasierte Zugriffssteuerungsregeln ein:

1. Aktivieren Sie die Funktion. Siehe ***Aktivieren der Funktion*** (auf Seite 117).
2. Legen Sie die Standardrichtlinie fest. Siehe ***Ändern der Standardrichtlinie*** (auf Seite 117).
3. Erstellen Sie Regeln, um anzugeben, welche Adressen zugelassen oder abgelehnt werden, wenn die Adressen mit einer bestimmten Benutzerfunktion assoziiert sind. Siehe ***Erstellen von benutzerfunktionsbasierten Zugriffssteuerungsregeln*** (auf Seite 118).

Die Änderungen werden für aktuell angemeldete Benutzer erst bei der nächsten Anmeldung wirksam.

Aktivieren der Funktion

Sie müssen diese Funktion für die Zugriffssteuerung aktivieren, bevor eine relevante Regel wirksam werden kann.

So aktivieren Sie benutzerfunktionsbasierte Zugriffssteuerungsregeln:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. Um die IPv4-Firewall zu aktivieren, klicken Sie auf die Registerkarte "IPv4", und aktivieren Sie das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv4 aktivieren).
3. Um die IPv6-Firewall zu aktivieren, klicken Sie auf die Registerkarte "IPv6", und aktivieren Sie das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren).
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Ändern der Standardrichtlinie

Unter der Standardrichtlinie wird sämtlicher Datenverkehr von allen IP-Adressen zugelassen, unabhängig davon, welche Benutzerfunktion dem Benutzer zugewiesen wurde.

So ändern Sie die Standardrichtlinie:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. So legen Sie die Standardrichtlinie für IPv4-Adressen fest:
   a. Klicken Sie ggf. auf die Registerkarte "IPv4".
   b. Stellen Sie sicher, dass das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv4 aktivieren) aktiviert ist.
   c. Wählen Sie in der Dropdown-Liste "Default Policy" (Standardrichtlinie) die gewünschte Aktion aus.

- Allow (Zulassen): Lässt Verkehr von allen IPv4-Adressen zu, unabhängig von der Benutzerfunktion.
- Deny (Ablehnen): Lehnt den Verkehr von allen IPv4-Adressen ab, unabhängig von der Benutzerfunktion.

3. So legen Sie die Standardrichtlinie für IPv6-Adressen fest:
   a. Klicken Sie auf die Registerkarte "IPv6".
   b. Stellen Sie sicher, dass das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren) aktiviert ist.
   c. Wählen Sie in der Dropdown-Liste "Default Policy" (Standardrichtlinie) die gewünschte Aktion aus.
      - Allow (Zulassen): Lässt Verkehr von allen IPv6-Adressen zu, unabhängig von der Benutzerfunktion.
      - Deny (Ablehnen): Lehnt den Verkehr von allen IPv6-Adressen ab, unabhängig von der Benutzerfunktion.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Erstellen von benutzerfunktionsbasierten Zugriffssteuerungsregeln

Mit benutzerfunktionsbasierten Zugriffssteuerungsregeln wird der Datenverkehr auf der Grundlage der Benutzerfunktion und der IP-Adresse des Benutzers zugelassen oder abgelehnt. Wie bei Firewall-Regeln ist auch hier die Reihenfolge der Regeln wichtig, da die Ausführung in numerischer Reihenfolge erfolgt.

So erstellen Sie benutzerfunktionsbasierte Zugriffssteuerungsregeln:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4" zum Erstellen von Firewall-Regeln, oder klicken Sie auf die Registerkarte "IPv6" zum Erstellen von IPv6-Firewall-Regeln.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Rollenbasierte Zugriffssteuerung für IPv4 aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Erstellen Sie spezifische Regeln:

Aktion	Vorgehensweise

Eine Regel am Ende der Regelliste anfügen	▪ Klicken Sie auf "Append" (Anfügen). Das Dialogfeld "Append new Rule" (Neue Regel anhängen) wird angezeigt.
	▪ Geben Sie im Feld "Starting IP Address" (IP-Startadresse) eine IP-Startadresse ein.
	▪ Geben Sie im Feld "Ending IP Address" (IP-Endadresse) eine IP-Endadresse ein.
	▪ Wählen Sie aus der Dropdown-Liste im Feld "Role" (Benutzerfunktion) eine Benutzerfunktion aus. Diese Regel gilt nur für Mitglieder dieser Benutzerfunktion.
	▪ Wählen Sie in der Dropdown-Liste im Feld "Policy" (Richtlinie) entweder "Allow" (Zulassen) oder "Deny" (Ablehnen) aus.
	  ▪ Allow (Zulassen): Lässt den Verkehr von dem angegebenen IP-Adressbereich zu, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist
	  ▪ Deny (Ablehnen): Lehnt den Verkehr von dem angegebenen IP-Adressbereich ab, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist
	▪ Klicken Sie auf "OK", um die Änderungen zu speichern.
	Der Regel wird automatisch vom System eine Nummer zugewiesen.

Eine Regel zwischen zwei vorhandenen Regeln einfügen	▪ Wählen Sie die Regel aus, über der Sie eine neue Regel einfügen möchten. Wenn Sie z. B. zwischen den Regeln 3 und 4 eine Regel einfügen möchten, wählen Sie 4 aus. ▪ Klicken Sie auf "Insert" (Einfügen). Das Dialogfeld "Insert new Rule" (Neue Regel einfügen) wird angezeigt. ▪ Geben Sie im Feld "Starting IP Address" (IP-Startadresse) eine IP-Startadresse ein. ▪ Geben Sie im Feld "Ending IP Address" (IP-Endadresse) eine IP-Endadresse ein. ▪ Wählen Sie aus der Dropdown-Liste im Feld "Role" (Benutzerfunktion) eine Benutzerfunktion aus. Diese Regel gilt nur für Mitglieder dieser Benutzerfunktion. ▪ Wählen Sie in der Dropdown-Liste im Feld "Policy" (Richtlinie) entweder "Allow" (Zulassen) oder "Deny" (Ablehnen) aus.

Aktion	Vorgehensweise
	▪ Allow (Zulassen): Lässt den Verkehr von dem angegebenen IP-Adressbereich zu, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist ▪ Deny (Ablehnen): Lehnt den Verkehr von dem angegebenen IP-Adressbereich ab, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist ▪ Klicken Sie auf "OK", um die Änderungen zu speichern. Das System fügt die Regel ein und nummeriert die folgenden Regeln automatisch neu.

5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Bearbeiten von benutzerfunktionsbasierten Zugriffssteuerungsregeln

Sie können bestehende Regeln ändern, wenn diese Regeln nicht ihren Anforderungen entsprechen.

So ändern Sie eine benutzerfunktionsbasierte Zugriffssteuerungsregel:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu ändern. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu ändern.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Rollenbasierte Zugriffssteuerung für IPv4 aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Wählen Sie die zu ändernde Regel in der Regelliste aus.
5. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf die Regel. Das Dialogfeld "Edit Rule" (Regel bearbeiten) wird eingeblendet.
6. Nehmen Sie an den angezeigten Informationen die Änderungen vor.
7. Klicken Sie auf "OK", um die Änderungen zu speichern.

Sortieren von benutzerfunktionsbasierten Zugriffssteuerungsregeln

Ähnlich wie bei Firewall-Regeln bestimmt die Reihenfolge der benutzerfunktionsbasierten Zugriffsteuerungsregeln, welche Regel, die mit der IP-Adresse übereinstimmt, ausgeführt wird.

So sortieren Sie benutzerfunktionsbasierte Zugriffssteuerungsregeln:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu sortieren. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu sortieren.
3. Achten Sie darauf, dass das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Rollenbasierte Zugriffssteuerung für IPv4 aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Klicken Sie auf eine bestimmte Regel, um sie auszuwählen.
5. Klicken Sie auf oder , um die ausgewählte Regel nach oben oder unten zu verschieben, bis sie die gewünschte Position in der Reihenfolge erreicht hat.
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen von benutzerfunktionsbasierten Zugriffssteuerungsregeln

Wenn eine Regel für die Zugriffssteuerung unnötig oder veraltet ist, entfernen Sie sie.

So löschen Sie eine benutzerfunktionsbasierte Zugriffssteuerungsregel:

1. Wählen Sie "Device Settings" > "Security" > "Role Based Access Control" (Geräteeinstellungen > Sicherheit > benutzerfunktionsbasierte Zugriffssteuerung) aus. Das Dialogfeld "Configure Role Bases Access Control Settings" (Einstellungen für die benutzerfunktionsbasierte Zugangssteuerung konfigurieren) wird angezeigt.
2. Klicken Sie auf die Registerkarte "IPv4", um die IPv4-Firewall-Regeln zu löschen. Klicken Sie auf die Registerkarte "IPv6", um die IPv6-Firewall-Regeln zu löschen.

3. Achten Sie darauf, dass das Kontrollkästchen "Enable Role Based Access Control for IPv4" (Rollenbasierte Zugriffssteuerung für IPv4 aktivieren) auf der Registerkarte "IPv4" oder das Kontrollkästchen "Enable Role Based Access Control for IPv6" (Benutzerfunktionsbasierte Zugriffssteuerung für IPv6 aktivieren) auf der Registerkarte "IPv6" aktiviert ist.
4. Wählen Sie die zu löschende Regel in der Regelliste aus. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
5. Klicken Sie auf "Delete" (Löschen).
6. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
7. Klicken Sie auf "OK", um die Änderungen zu speichern.

Einrichten eines SSL-Zertifikats

Mit einem digitalen X.509-Zertifikat wird die Identität beider Parteien in einer SSL-Verbindung überprüft.

Um für die EMX-Einheit ein Zertifikat zu beantragen, müssen Sie ein Certificate Signing Request (CSR) erstellen und einer Zertifizierungsinstanz (CA) zusenden. Sobald die Zertifizierungsinstanz die Informationen im CSR verarbeitet hat, erhalten Sie ein SSL-Zertifikat, dass Sie auf dem EMX-Gerät installieren müssen.

Hinweis: Informationen zum Erzwingen von SSL bei der Verbindung mit der EMX-Einheit finden Sie unter **Erzwingen der HTTPS-Verschlüsselung** *(auf Seite 104).*

Ein CSR ist in folgenden Fällen nicht erforderlich:

- Sie möchten ein *selbstsigniertes* Zertifikat auf dem EMX-Gerät erstellen.
- Entsprechendes, gültiges Zertifikat und Schlüsseldateien sind verfügbar.

Certificate Signing Request (CSR)

Wenn für die EMX-Einheit kein geeignetes Zertifikat und keine Schlüsseldateien verfügbar sind, können Sie auf dem EMX-Gerät einen CSR sowie einen privaten Schlüssel erstellen und den CSR zum Signieren des Zertifikats an die Zertifizierungsinstanz senden.

Erstellen eines Certificate Signing Request (CSR)

Führen Sie die folgenden Schritte aus, um das CSR für das EMX-Gerät zu erstellen.

So erstellen Sie ein CSR:

1. Wählen Sie "Device Settings" > "Security" > "SSL Certificate" (Geräteeinstellungen > Sicherheit > SSL-Zertifikat) aus. Das Dialogfeld "Manage SSL Certificate" (SSL-Zertifikat verwalten) wird angezeigt.
2. Klicken Sie auf die Registerkarte "New SSL Certificate" (Neues SSL-Zertifikat).
3. Geben Sie die erforderlichen Informationen
   - Im Bereich "Subject" (Betreff):

Feld	Geben Sie diese Informationen ein
Country (ISO Code) (Land [ISO-Code])	Land, in dem Ihr Unternehmen ansässig ist. Verwenden Sie den Standard-ISO-Ländercode. Eine Liste der ISO-Codes finden Sie auf der ***ISO-Website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province (Bundesland oder Region)	Vollständiger Name des Bundeslands/der Region, in dem bzw. der Ihr Unternehmen ansässig ist
Locality (Ort)	Ort/Stadt, in dem bzw. der Ihr Unternehmen ansässig ist
Organization (Organisation)	Registrierter Name Ihres Unternehmens
Organizational Unit (Organisationseinheit)	Name Ihrer Abteilung
Common Name (Allgemeiner Name)	Vollständig qualifizierter Domänenname (FQDN) des EMX-Geräts.
Email address (E-Mail-Adresse)	E-Mail-Adresse, unter der Sie oder ein anderer Benutzer mit Administratorrechten erreichbar sind bzw. ist

Hinweis: Alle Felder im Bereich "Subject" (Betreff), ausgenommen "Organization" (Organisation), "Organizational Unit" (Organisationseinheit) und "Email Address" (E-Mail-Adresse) sind obligatorisch. Wenn Sie ein CSR erstellen, ohne Werte in die erforderlichen Felder einzugeben, können Sie keine externen Zertifikate beantragen.

   - Im Bereich "Key Creation Parameters" (Parameter für Schlüsselerstellung):

Feld	Vorgehensweise
Schlüssellänge	Wählen Sie in der Dropdown-Liste in diesem Feld die Schlüssellänge (Bits) aus. Ein längerer Schlüssel erhöht die Sicherheit, verlangsamt jedoch die Reaktionszeit des EMX-Geräts.
Self Sign (Selbst signieren)	**Um ein von der Zertifizierungsinstanz signiertes Zertifikat anzufordern, darf dieses Kontrollkästchen NICHT aktiviert sein.**
Challenge	Geben Sie ein Kennwort ein. Das Kennwort wird zum Schützen des Zertifikats oder CSR verwendet. Diese Informationen sind optional. Der Wert muss zwischen 4 bis 64 Zeichen lang sein. Beim Kennwort ist die Groß-/Kleinschreibung zu beachten.
Confirm Challenge (Challenge bestätigen)	Geben Sie zur Bestätigung dasselbe Kennwort erneut ein.

4. Klicken Sie auf "Create New SSL Key" (Neuen SSL-Schlüssel erstellen), um den CSR und den privaten Schlüssel zu erstellen. Dies kann mehrere Minuten dauern.
5. Um das soeben erstellte CSR auf Ihren Computer herunterzuladen, klicken Sie auf "Download Certificate Signing Request" (CSR herunterladen).
   a. Sie werden zum Öffnen oder Speichern der Datei aufgefordert. Klicken Sie auf "Save" (Speichern), um es auf dem Computer zu speichern.
   b. Nachdem Sie die Datei auf Ihrem Computer gespeichert haben, senden Sie sie an eine Zertifizierungsinstanz, um das digitale Zertifikat anzufordern.
   c. Klicken Sie gegebenenfalls auf "Delete Certificate Signing Request" (CSR löschen), um die CSR-Datei permanent aus dem EMX-Gerät zu löschen.
6. Um den soeben erstellten privaten Schlüssel auf Ihrem Computer zu speichern, klicken Sie auf "Download". Sie werden zum Öffnen oder Speichern der Datei aufgefordert. Klicken Sie auf "Save" (Speichern), um es auf dem Computer zu speichern.
7. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Installieren eines von der Zertifizierungsinstanz signierten Zertifikats

Nachdem die Zertifizierungsinstanz ein signiertes Zertifikat gemäß dem von Ihnen gesendeten CSR bereitgestellt hat, müssen Sie es auf dem EMX-Gerät installieren.

So installieren Sie das Zertifikat:

1. Wählen Sie "Device Settings" > "Security" > "SSL Certificate" (Geräteeinstellungen > Sicherheit > SSL-Zertifikat) aus. Das Dialogfeld "Manage SSL Certificate" (SSL-Zertifikat verwalten) wird angezeigt.
2. Klicken Sie auf die Registerkarte "New SSL Certificate" (Neues SSL-Zertifikat).
3. Klicken Sie im Feld "Certificate File" (Zertifikatsdatei) auf "Browse" (Durchsuchen), um die von der Zertifizierungsinstanz bereitgestellte Zertifikatsdatei auszuwählen.
4. Klicken Sie auf "Upload" (Hochladen). Das Zertifikat wird auf dem EMX-Gerät installiert.

   Tipp: Klicken Sie auf die Registerkarte "Active SSL Certificate" (Aktives SSL-Zertifikat), um zu überprüfen, ob das Zertifikat erfolgreich installiert wurde.

5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Erstellen eines selbstsignierten Zertifikats

Wenn für das EMX-Gerät kein entsprechendes Zertifikat und keine Schlüsseldateien verfügbar sind, können Sie anstatt ein CSR an die Zertifizierungsinstanz zu senden ein selbstsigniertes Zertifikat erstellen.

So erstellen und installieren Sie ein selbstsigniertes Zertifikat:

1. Wählen Sie "Device Settings" > "Security" > "SSL Certificate" (Geräteeinstellungen > Sicherheit > SSL-Zertifikat) aus. Das Dialogfeld "Manage SSL Certificate" (SSL-Zertifikat verwalten) wird angezeigt.
2. Klicken Sie auf die Registerkarte "New SSL Certificate" (Neues SSL-Zertifikat).
3. Geben Sie die erforderlichen Informationen

Feld	Geben Sie diese Informationen ein
Country (ISO Code) (Land [ISO-Code])	Land, in dem Ihr Unternehmen ansässig ist. Verwenden Sie den Standard-ISO-Ländercode. Eine Liste der ISO-Codes finden Sie auf der ***ISO-Website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).

Feld	Geben Sie diese Informationen ein
State or Province (Bundesland oder Region)	Vollständiger Name des Bundeslands/der Region, in dem bzw. der Ihr Unternehmen ansässig ist
Locality (Ort)	Ort/Stadt, in dem bzw. der Ihr Unternehmen ansässig ist
Organization (Organisation)	Registrierter Name Ihres Unternehmens
Organizational Unit (Organisationseinheit)	Name Ihrer Abteilung
Common Name (Allgemeiner Name)	Vollständig qualifizierter Domänenname (FQDN) des EMX-Geräts.
Email address (E-Mail-Adresse)	E-Mail-Adresse, unter der Sie oder ein anderer Benutzer mit Administratorrechten erreichbar sind bzw. ist
Schlüssellänge	Wählen Sie in der Dropdown-Liste in diesem Feld die Schlüssellänge (Bits) aus. Ein längerer Schlüssel erhöht die Sicherheit, verlangsamt jedoch die Reaktionszeit des EMX-Geräts.
Self Sign (Selbst signieren)	**Dieses Kontrollkästchen muss aktiviert sein, damit Sie ein selbstsigniertes Zertifikat erstellen können.**
Validity in days (Gültigkeit in Tagen)	Dieses Feld wird angezeigt, nachdem Sie das Kontrollkästchen "Self Sign" (Selbst signieren) aktiviert haben. Geben Sie die Anzahl der Tage ein, für die das selbstsignierte Zertifikat gültig ist.

Hinweis: Alle Felder im Bereich "Subject" (Betreff), ausgenommen "Organization" (Organisation), "Organizational Unit" (Organisationseinheit) und "Email Address" (E-Mail-Adresse) sind obligatorisch.

Für ein selbstsigniertes Zertifikat ist kein Kennwort erforderlich, d. h. die Felder "Challenge" und "Confirm Challenge" (Challenge bestätigen) werden ausgeblendet, nachdem das Kontrollkästchen "Self Sign" (Selbst signieren) aktiviert wurde.

4. Klicken Sie auf "Create New SSL Key" (Neuen SSL-Schlüssel erstellen), um das selbstsignierte Zertifikat und den privaten Schlüssel zu erstellen. Dies kann mehrere Minuten dauern.
5. Sie können auch einen der folgenden Schritte ausführen:
   - Klicken Sie auf "Install Key and Certificate" (Schlüssel und Zertifikat installieren), um das selbstsignierte Zertifikat und den privaten Schlüssel sofort zu installieren. Wenn Bestätigungs- und Sicherheitsmeldungen angezeigt werden, klicken Sie auf "Yes" (Ja), um fortzufahren.

Tipp: Klicken Sie auf die Registerkarte "Active SSL Certificate" (Aktives SSL-Zertifikat), um zu überprüfen, ob das Zertifikat erfolgreich installiert wurde.

- Um das selbstsignierte Zertifikat oder den privaten Schlüssel herunterzuladen, klicken Sie auf "Download Certificate" (Zertifikat herunterladen) oder "Download Key" (Schlüssel herunterladen). Sie werden zum Öffnen oder Speichern der Datei aufgefordert. Klicken Sie auf "Save" (Speichern), um es auf dem Computer zu speichern.
- Um das selbstsignierte Zertifikat und den privaten Schlüssel permanent vom EMX-Gerät zu löschen, klicken Sie auf "Delete Key and Certificate" (Schlüssel und Zertifikat löschen).

6. Wenn Sie in Schritt 5 das selbstsignierte Zertifikat installiert haben, wird das EMX-Gerät zurückgesetzt und die Anmeldeseite erneut angezeigt, nachdem der Installationsvorgang abgeschlossen ist.

Installieren vorhandener Schlüssel- und Zertifikatsdateien

Wenn die SSL-Zertifikats- und private Schlüsseldatei bereits verfügbar sind, können Sie sie direkt installieren, ohne einen CSR oder ein selbstsigniertes Zertifikat zu erstellen.

So installieren Sie vorhandene Schlüssel- und Zertifikatsdateien:

1. Wählen Sie "Device Settings" > "Security" > "SSL Certificate" (Geräteeinstellungen > Sicherheit > SSL-Zertifikat) aus. Das Dialogfeld "Manage SSL Certificate" (SSL-Zertifikat verwalten) wird angezeigt.
2. Klicken Sie auf die Registerkarte "New SSL Certificate" (Neues SSL-Zertifikat).
3. Aktivieren Sie das Kontrollkästchen "Upload Key and Certificate" (Schlüssel und Zertifikat hochladen). Die Felder "Key File" (Schlüsseldatei) und "Certificate File" (Zertifikatsdatei) werden angezeigt.
4. Klicken Sie im Feld "Key File" (Schlüsseldatei) auf "Browse" (Durchsuchen), um die private Schlüsseldatei auszuwählen.
5. Klicken Sie im Feld "Certificate File" (Zertifikatsdatei) auf "Browse" (Durchsuchen), um die Zertifikatsdatei auszuwählen.
6. Klicken Sie auf "Upload" (Hochladen). Die ausgewählten Dateien werden auf dem EMX-Gerät installiert.

Tipp: Klicken Sie auf die Registerkarte "Active SSL Certificate" (Aktives SSL-Zertifikat), um zu überprüfen, ob das Zertifikat erfolgreich installiert wurde.

7. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Herunterladen von Schlüssel- und Zertifikatsdateien

Sie können die aktuell auf dem EMX-Gerät installierten Schlüssel- und Zertifikatsdateien für Datensicherungen oder andere Vorgänge herunterladen. Sie können z. B. die Dateien auf einem EMX-Ersatzgerät installieren, das Zertifikat zu Ihrem Browser hinzufügen usw.

So laden Sie die Zertifikats- und Schlüsseldateien von einem EMX-Gerät herunter:

1. Wählen Sie "Device Settings" > "Security" > "SSL Certificate" (Geräteeinstellungen > Sicherheit > SSL-Zertifikat) aus. Das Dialogfeld "Manage SSL Certificate" (SSL-Zertifikat verwalten) wird angezeigt.
2. Die Registerkarte "Active SSL Certificate" (Aktives SSL-Zertifikat) sollte geöffnet sein. Falls nicht, klicken Sie auf diese Registerkarte.
3. Klicken Sie auf "Download Key" (Schlüssel herunterladen), um die auf dem EMX-Gerät installierte private Schlüsseldatei herunterzuladen. Sie werden zum Öffnen oder Speichern der Datei aufgefordert. Klicken Sie auf "Save" (Speichern), um es auf dem Computer zu speichern.
4. Klicken Sie auf "Download Certificate" (Zertifikat herunterladen), um die auf dem EMX-Gerät installierte Zertifikatsdatei herunterzuladen. Sie werden zum Öffnen oder Speichern der Datei aufgefordert. Klicken Sie auf "Save" (Speichern), um es auf dem Computer zu speichern.
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Einrichten der LDAP-Authentifizierung

Aus Sicherheitsgründen müssen Benutzer, die versuchen, sich bei der EMX-Einheit anzumelden, authentifiziert werden. Die EMX-Einheit unterstützt den Zugriff mithilfe einer der folgenden Authentifizierungsmechanismen:

- Lokale Datenbank mit Benutzerprofilen auf dem EMX-Gerät
- LDAP (Lightweight Directory Access Protocol)

Die EMX-Einheit ist standardmäßig für die lokale Authentifizierung konfiguriert. Wenn Sie bei dieser Methode bleiben möchten, müssen Sie lediglich für jeden autorisierten Benutzer ein Benutzerprofil erstellen. Wenn Sie einen externen LDAP-Server bevorzugen, müssen Sie Folgendes ausführen:

- Geben Sie die Informationen zum LDAP-Server für die EMX-Einheit an.
- Erstellen Sie Benutzerprofile für Benutzer, die extern authentifiziert werden, da ein Benutzerprofil auf dem EMX-Gerät die Benutzerfunktion(en), die dem Benutzer zugewiesen sind, sowie die entsprechenden Berechtigungen für den Benutzer festlegt.

Wenn die LDAP-Authentifizierung aktiviert ist, müssen alle EMX-Benutzer ein Konto auf dem LDAP-Server aufweisen. Benutzer, für die nur die lokale Authentifizierung eingerichtet ist, haben keinen Zugriff auf die EMX-Einheit. Ausgenommen hiervon ist der Administrator, der immer auf die EMX-Einheit zugreifen kann.

Ermitteln der LDAP-Informationen

Zum Konfigurieren der EMX-Einheit für die LDAP-Authentifizierung sind spezielle Kenntnisse über LDAP-Server und Verzeichniseinstellungen erforderlich. Wenn Sie sich mit den Einstellungen nicht auskennen, wenden Sie sich an Ihren LDAP-Administrator.

Um die LDAP-Authentifizierung zu konfigurieren, müssen Sie Folgendes prüfen:

- IP-Adresse oder Hostname des LDAP-Servers
- Ob das sichere LDAP-Protokoll (LDAP mit SSL) verwendet wird
  - Wenn das sichere LDAP verwendet wird, fragen Sie Ihren LDAP-Administrator nach der CA-Zertifizierungsdatei.
- Netzwerkport, der vom LDAP-Server verwendet wird
- LDAP-Servertyp; normalerweise einer der Folgenden:
  - *OpenLDAP*

  - Wenn Sie einen OpenLDAP-Server verwenden, fragen Sie Ihren LDAP-Administrator nach dem DN (Bind Distinguished Name) und Kennwort.
- *Microsoft Active Directory® (AD)*
  - Bei Verwendung eines Microsoft Active Directory-Servers fragen Sie Ihren AD-Administrator nach dem Namen der Active Directory-Domäne.

- Bind Distinguished Name (DN) und Kennwort (wenn Anonymous Bind NICHT verwendet wird)
- Basis-DN des Servers (wird zur Suche nach Benutzern verwendet)
- Anmeldeattribut (oder AuthorizationString)
- Objektklasse für Benutzereinträge
- Subfilter für Benutzersuche (oder BaseSearch)

Hinzufügen der LDAP-Servereinstellungen

Um die externen LDAP/LDAPS-Serverauthentifizierung zu aktivieren und zu verwenden, aktivieren Sie die LDAP-Authentifizierung und geben die Informationen ein, die Sie für den LDAP/LDAPS-Server ermittelt haben.

Hinweis: Ein LDAPS-Server bezieht sich auf einen SSL-sicheren LDAP-Server.

So fügen Sie die LDAP/LDAPS-Servereinstellungen hinzu:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie das Optionsfeld "LDAP" aus, um die LDAP/LDAPS-Remote-Serverauthentifizierung zu aktivieren.
3. Klicken Sie auf "New" (Neu), um einen LDAP/LDAPS-Server für die Authentifizierung hinzuzufügen. Das Dialogfeld "Create new LDAP Server Configuration" (Neue LDAP-Serverkonfiguration erstellen) wird angezeigt.
4. IP-Adresse / Hostname – Geben Sie die IP-Adresse oder den Hostnamen des LDAP/LDAPS-Authentifizierungsservers ein.

   Wichtig: Wenn die SSL-Verschlüsselung deaktiviert ist, können Sie entweder den Domänennamen oder die PI-Adresse in dieses Feld eingeben. Wenn die SSL-Verschlüsselung aktiviert ist, müssen Sie den vollständig qualifizierten Domänennamen eingeben.
5. Typ des externen LDAP-/LDAPS-Servers. Wählen Sie eine der verfügbaren Optionen aus:
   - OpenLDAP

- Microsoft Active Directory Active Directory ist eine Implementierung von LDAP-/LDAPS-Verzeichnistdiensten von Microsoft zur Verwendung in Windows-Umgebungen.

6. LDAP over SSL (LDAP über SSL) – Aktivieren Sie dieses Kontrollkästchen, wenn Sie SSL verwenden möchten. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, mit dem EMX sicher mit dem LDAP-/LDAPS-Server kommunizieren kann.
7. Port – Der Standardport lautet 389. Verwenden Sie entweder den Standard-LDAP-TCP-Port oder geben Sie einen anderen Port an.
8. SSL Port – Die Standardeinstellung ist 636. Verwenden Sie entweder den Standardport, oder geben Sie einen anderen Port an. Dieses Feld ist aktiviert, wenn das Kontrollkästchen "LDAP over SSL" (LDAP über SSL) aktiviert wurde.
9. Use only trusted LDAP Server Certificates (Nur als vertrauenswürdig eingestufte LDAP-Serverzertifikate verwenden) – Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine vertrauenswürdige LDAP-Serverzertifikatsdatei verwenden möchten, d. h. eine von der Zertifizierungsinstanz signierte Zertifikatsdatei. Wenn dieses Kontrollkästchen NICHT aktiviert ist, können Sie alle LDAP/LDAPS-Serverzertifikate verwenden, einschließlich einer selbstsignierten Zertifikatsdatei. Nachdem diese Option aktiviert wurde, ist eine Zertifikatsdatei erforderlich.
10. Server Certificate (Serverzertifikat) – Wenden Sie sich an den Administrator des Authentifizierungsservers, um die CA-Zertifikatsdatei für den LDAP-/LDAPS-Server zu erhalten. Verwenden Sie die Schaltfläche "Browse" (Durchsuchen), um zur Zertifikatdatei zu navigieren. Diese Datei ist erforderlich, wenn das Kontrollkästchen "Use only trusted LDAP Server Certificates" (Nur als vertrauenswürdig eingestufte LDAP-Serverzertifikate verwenden) aktiviert ist.

Tipp: Sie können die CA-Zertifikatsdatei zur späteren Verwendung zunächst hochladen und das Kontrollkästchen "Use only trusted LDAP Server Certificates" (Nur als vertrauenswürdig eingestufte LDAP-Serverzertifikate verwenden) erst dann aktivieren, wenn Sie die Zertifikatsdatei benötigen.

---

11. Anonymous Bind - Für "OpenLDAP", verwenden Sie dieses Kontrollkästchen, um Anonymous Bind zu aktivieren oder zu deaktivieren.
    - Aktivieren Sie das Kontrollkästchen, um Anonymous Bind zu verwenden.
    - Wenn ein Bind-DN und -Kennwort erforderlich sind, um eine Anbindung zu dem externen LDAP-/LDAPS-Server herzustellen, heben Sie die Markierung für dieses Kontrollkästchen auf.
12. Bind-Berechtigungsnachweise verwenden - Verwenden Sie für "Microsoft Active Directory" dieses Kontrollkästchen, um Anonymous Bind zu aktivieren oder zu deaktivieren.

- Deaktivieren Sie das Kontrollkästchen, um Anonymous Bind zu verwenden. Standardmäßig ist das Kontrollkästchen deaktiviert.
- Wenn ein Bind-DN und -Kennwort erforderlich sind, um eine Anbindung zu dem externen LDAP-/LDAPS-Server herzustellen, markieren Sie dieses Kontrollkästchen.

13. Bind DN – Geben Sie den DN des Benutzers an, der die Berechtigung zum Durchsuchen des LDAP-Verzeichnisses in der definierten Suchdatenbank aufweist. Diese Information wird nur benötigt, wenn das Kontrollkästchen "Use Bind Credentials" (Bind-Berechtigungsnachweise verwenden) markiert ist.
14. Bind Password and Confirm Bind Password (Bind-Kennwort und Bind-Kennwort bestätigen) – Geben Sie das Bind-Kennwort zuerst im Feld "Bind Password" (Bind-Kennwort) und anschließend im Feld "Confirm Bind Password" (Bind-Kennwort bestätigen) ein. Diese Information wird nur benötigt, wenn das Kontrollkästchen "Use Bind Credentials" (Bind-Berechtigungsnachweise verwenden) markiert ist.
15. Base DN for Search (Basis-DN für Suche) – Geben Sie den Namen ein, den Sie mit dem LDAP-/LDAPS-Server verknüpfen möchten (bis zu 31 Zeichen), und wo in der Datenbank die Suche nach dem angegebenen Basis-DN begonnen werden soll. Ein Wert für die Basissuche kann beispielsweise folgendermaßen aussehen: `cn=Users,dc=raritan,dc=com`. Wenden Sie sich an den Administrator des Authentifizierungsservers, um die entsprechenden Werte zur Eingabe in diese Felder zu erhalten.
16. Geben Sie die folgenden Informationen in den entsprechenden Feldern ein. Der LDAP-Server benötigt diese Informationen zur Überprüfung von Benutzernamen und Kennwörtern.
    - Login name attribute (Anmeldeattribut; auch als "AuthorizationString" bezeichnet)
    - **Name of user-entry object class** (Name der Objektklasse für Benutzereinträge)
    - User Search Subfilter (Subfilter für Benutzersuche; auch als "BaseSearch" bezeichnet)

    Hinweis: Die EMX-Einheit gibt das Anmeldeattribut und die Objektklasse für Benutzereinträge mit Standardwerten vorab an. Diese sollten nicht geändert werden, sofern dies nicht erforderlich ist.
17. Active Directory Domain (Active Directory-Domäne) – Geben Sie den Namen der Active Directory-Domäne ein, z. B. "testradius.com". Fragen Sie Ihren Active Directory-Administrator nach dem jeweiligen Domänennamen.
18. Um zu überprüfen, ob die LDAP/LDAPS-Konfiguration ordnungsgemäß funktioniert, klicken Sie auf "Test Connection" (Verbindung testen), um zu überprüfen, ob die EMX-Einheit eine Verbindung zum LDAP/LDAPS-Server herstellen kann.

Tipp: Sie können dies auch testen, indem Sie im Dialogfeld "Authentication Settings" auf die Schaltfläche "Test Connection" (Verbindung testen) klicken.

19. Klicken Sie auf "OK", um die Änderungen zu speichern. Der neue LDAP-Server wird im Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) aufgeführt.
20. Um weitere LDAP/LDAPS-Server hinzuzufügen, wiederholen Sie die Schritte 3 bis 19.
21. Klicken Sie auf "OK", um die Änderungen zu speichern. Die LDAP-Authentifizierung ist nun konfiguriert.

Hinweis: Wenn die Uhr von EMX und die des LDAP-Servers nicht mehr synchronisiert sind, werden die Zertifikate als abgelaufen betrachtet und die Benutzer können nicht mithilfe von LDAP authentifiziert werden. Um eine ordnungsgemäße Synchronisierung sicherzustellen, sollten Administratoren die EMX-Einheit und den LDAP-Server so konfigurieren, dass sie denselben NTP-Server verwenden.

Weitere Informationen zur AD-Konfiguration

Weitere Informationen zur LDAP-Konfiguration mithilfe von Microsoft Active Directory finden Sie unter ***Veranschaulichung der LDAP-Konfiguration*** (auf Seite 344).

Sortieren der Reihenfolge für den LDAP-Zugriff

Die Reihenfolge der LDAP-Liste legt die Zugriffspriorität der Remote-LDAP/LDAPS-Server fest. Die EMX-Einheit versucht zuerst, auf den in der Liste zuerst angezeigten LDAP/LDAPS-Server für die Authentifizierung zuzugreifen. Anschließend wird auf den nächsten Server zugegriffen, falls der Zugriff auf den ersten Server nicht erfolgreich war usw. Dies erfolgt solange, bis das EMX-Gerät eine Verbindung zu einem LDAP/LDAPS-Server in der Liste herstellen kann.

Hinweis: Nach der erfolgreichen Verbindung zu einem LDAP/LDAPS-Server greift die EMX-Einheit NICHT mehr auf die verbleibenden LDAP/LDAPS-Server in der Liste zu. Das Ergebnis der Benutzerauthentifizierung wird dabei nicht berücksichtigt.

So sortieren Sie die Liste für den LDAP-Serverzugriff neu:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie den LDAP/LDAPS-Server aus, dessen Priorität Sie ändern möchten.

3. Klicken Sie auf "Move up" (Nach oben verschieben) oder "Move down" (Nach unten verschieben), um den ausgewählten Server an die entsprechende Position in der Liste zu verschieben.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Testen der LDAP-Serververbindung

Sie können die Verbindung zu einem beliebigen LDAP/LDAPS-Server testen, um den Serverzugriff oder die Gültigkeit der Authentifizierungseinstellungen zu überprüfen.

So testen Sie die Verbindung zu einem LDAP/LDAPS-Server:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie den LDAP/LDAPS-Server aus, den Sie testen möchten.
3. Klicken Sie auf "Test Connection" (Verbindung testen), um den Verbindungstest zu starten.

Bearbeiten der LDAP-Servereinstellungen

Wenn die Konfiguration auf einem LDAP/LDAPS-Server geändert wurde, wie z. B. Portnummer, Bind-DN und -Kennwort, müssen Sie die LDAP/LDAPS-Einstellungen auf dem EMX-Gerät entsprechend anpassen. Andernfalls tritt ein Fehler bei der Authentifizierung auf.

So ändern Sie die LDAP-Authentifizierungskonfiguration:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie den LDAP/LDAPS-Server aus, den Sie bearbeiten möchten.
3. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "Edit LDAP Server Configuration" (LDAP-Serverkonfiguration bearbeiten) wird angezeigt.
4. Nehmen Sie an den angezeigten Informationen die erforderlichen Änderungen vor.
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen der LDAP-Servereinstellungen

Sie können die Authentifizierungseinstellungen für einen bestimmten LDAP/LDAPS-Server löschen, wenn der Server nicht verfügbar ist oder für die Remote-Authentifizierung verwendet wird.

So entfernen Sie einen oder mehrere LDAP-/LDAPS-Server:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie den LDAP/LDAPS-Server aus, den Sie entfernen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
3. Klicken Sie auf "Delete" (Löschen).
4. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Deaktivieren der LDAP-Authentifizierung

Wenn der Remote-Authentifizierungsdienst deaktiviert ist, authentifiziert die EMX-Einheit die Benutzer anhand der auf dem EMX-Gerät gespeicherten lokalen Datenbank.

So deaktivieren Sie den LDAP-Authentifizierungsdienst:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie das Optionsfeld "Local Authentication" (Lokale Authentifizierung) aus.
3. Klicken Sie auf "OK", um die Änderungen zu speichern.

Aktivieren der LDAP- und lokalen Authentifizierungsdienste

Damit eine Authentifizierung immer ordnungsgemäß funktioniert, selbst wenn eine externe Authentifizierung nicht verfügbar ist, können Sie die lokalen und Remote-Authentifizierungsdienste aktivieren.

Wenn beide Authentifizierungsdienste aktiviert sind, hält die EMX-Einheit die folgenden Regeln für die Authentifizierung ein:

- Wenn ein LDAP/LDAPS-Server in der Zugriffsliste zur Verfügung steht, führt die EMX-Einheit die Authentifizierung nur am verbundenen LDAP/LDAPS-Server aus.
- Wenn die Verbindung zu allen LDAP/LDAPS-Servern fehlschlägt, ermöglicht die EMX-Einheit eine Authentifizierung anhand der lokalen Datenbank.

So aktivieren Sie beide Authentifizierungsdienste:

1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Das Optionsfeld "LDAP" muss ausgewählt sein.
3. Aktivieren Sie das Kontrollkästchen "Use Local Authentication if Remote Authentication service is not available" (Lokale Authentifizierung verwenden, wenn Remote-Authentifizierungsdienst nicht verfügbar ist).
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Kapitel 7 Ereignisregeln, Ereignisaktionen und Anwendungsprotokolle

In diesem Kapitel

Ereignisregeln und Aktionen.....137
Ereignisprotokollierung.....166
Anzeigen des Kommunikationsprotokolls.....168

Ereignisregeln und Aktionen

Ein Vorteil des intelligenten Produkts besteht in der Fähigkeit, Sie über Bedingungsänderungen zu benachrichtigen und darauf zu reagieren. Diese Ereignisbenachrichtigung oder Reaktion ist eine "Ereignisregel".

Auf der EMX-Einheit sind zwei Ereignisregeln vordefiniert, die nicht gelöscht werden können.

- Regel für das Systemereignisprotokoll: Mithilfe dieser Regel wird JEDES Ereignis in der EMX-Einheit im internen Protokoll aufgezeichnet. Die Regel ist standardmäßig aktiviert.
- Regel für System-SNMP-Trap: Mithilfe dieser Regel werden SNMP-Traps an die angegebenen IP-Adressen oder Hosts gesendet, sobald ein BELIEBIGES Ereignis in der EMX-Einheit stattfindet. Die Regel ist standardmäßig deaktiviert.

Falls diese beiden für Ihre Bedürfnisse nicht ausreichen, können Sie zusätzliche Regeln erstellen, um auf andere Ereignisse zu reagieren.

Hinweis: Internet Explorer® 8 (IE8) verwendet kein kompiliertes JavaScript. Wenn Sie zum Erstellen oder Ändern von Ereignisregeln IE8 verwenden, kann die Leistung der CPU beeinträchtigt sein, was zur Anzeige der Meldung über die Zeitüberschreitung der Verbindung führt. Klicken Sie in diesem Fall auf "Ignore" (Ignorieren), um fortzufahren.

Komponenten einer Ereignisregel

Eine Ereignisregel definiert die Reaktion der EMX-Einheit in bestimmten Situationen und besteht aus zwei Komponenten:

- Event (Ereignis): Dies ist die Situation, in der die EMX-Einheit oder eine Komponente eine bestimmte Bedingung feststellt. Beispielsweise übersteigt der Temperatursensor den Warnschwellenwert.
- Aktion: Dies ist die Antwort auf das Ereignis. Beispielsweise informiert die EMX-Einheit den Systemadministrator über das Ereignis und zeichnet es im Protokoll auf.

Hinweis: Ereignisregeln für Asset-Management-Sensoren müssen nach einem EMX-Firmware-Upgrade neu erstellt werden.

Erstellen einer Ereignisregel

Um eine Gruppe neuer Ereignisregeln zu erstellen, führen Sie nacheinander die folgenden Schritte aus:

- Erstellen Sie Aktionen für die Reaktion auf ein oder mehrere Ereignisse.
- Erstellen Sie Regeln, die bestimmen, welche Aktion bei Auftreten dieser Ereignisse ausgeführt werden soll.

Erstellen von Regeln

Wenn notwendige Aktionen verfügbar sind, können Sie Ereignisregeln erstellen, um festzulegen, welche Aktionen als Reaktion auf bestimmte Ereignisse ausgeführt werden sollen.

Die EMX-Einheit verfügt standardmäßig über zwei integrierte Ereignisregeln: "System Event Log Rule" (Systemereignisprotokoll-Regel) und "System SNMP Trap Rule" (System-SNMP-Trap-Regel). Wenn die integrierten Regeln nicht Ihre Anforderungen erfüllen sollten, können Sie neue Regeln erstellen.

So erstellen Sie Ereignisregeln:

1. Wählen Sie "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln) aus. Das Fenster "Event Rule Settings" (Ereignisregeleinstellungen) wird eingeblendet.
2. Klicken Sie auf der Registerkarte "Rules" (Regeln) auf "New Rule" (Neue Regel).
3. Geben Sie in das Feld "Rule name" (Regelname) einen neuen Namen ein, der die Regel kennzeichnet. Der Standardname lautet "New Rule" (Neue Regel) <Nummer>, wobei <Nummer> einer laufenden Nummer entspricht.

4. Klicken Sie auf das Kontrollkästchen "Enabled" (Aktiviert), um diese Ereignisregel zu aktivieren.
5. Klicken Sie auf "Event" (Ereignis), um ein Ereignis auszuwählen, bei dem eine Aktion ausgelöst werden soll. Es wird ein Pulldown-Menü mit allen Arten von Ereignissen angezeigt.
   - Wählen Sie den gewünschten Ereignistyp aus dem Pulldown-Menü aus. Falls ein Untermenü angezeigt wird, fahren Sie mit der Navigation weiter fort, bis das gewünschte Ereignis ausgewählt ist.

Hinweis: Die Option <Any sub-event> (Beliebiges Unterereignis) bezieht sich auf alle Ereignisse/Elemente, die im selben Untermenü aufgelistet sind. <Any slot> (Beliebiger Slot) bezieht sich auf alle Slots, <Any server> (Beliebiger Server) bezieht sich auf alle Server und <Any user> (Beliebiger Benutzer) bezieht sich auf alle Benutzer.

6. Je nach dem von Ihnen im vorherigen Schritt ausgewählten Ereignis kann es sein, dass das Feld "Trigger condition" (Auslösebedingung) mit den drei Optionsfeldern nicht angezeigt wird.

Ereignistypen	Optionsfelder
Ereignisse mit Überschreiten der Schwellenwerte numerischer Sensoren oder Verbinden und Trennen von Asset-Tags	Verfügbare Optionsfelder sind "Asserted" (Assertion), "Deasserted" (Deassertion) und "Both" (Beides). ▪ Asserted (Assertion): Die EMX-Einheit führt die Aktion nur aus, wenn das Ereignis stattfindet. Dies bedeutet der Status des beschriebenen Ereignisses wird von FALSE (FALSCH) in TRUE (WAHR) geändert. ▪ Deasserted (Deassertion): Die EMX-Einheit führt die Aktion nur aus, wenn die Ereignisbedingung nicht mehr vorhanden ist. Dies bedeutet der Status des beschriebenen Ereignisses wird von TRUE (WAHR) in FALSE (FALSCH) geändert. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn das Ereignis stattfindet (Assertion) und die Ereignisbedingung nicht mehr vorhanden ist (Deassertion).

Ereignistypen	Optionsfelder
Statuswechsel des Einzelsensors (Ein/Aus)	Verfügbare Optionsfelder sind "Alarmed" (Alarmzustand), "No longer alarmed" (Alarmzustand vorbei) und "Both" (Beides). ▪ Alarmed (Alarmzustand): Die EMX-Einheit führt die Aktion nur aus, wenn der gewählte Sensor in den Alarmzustand, d.h. den abnormen Zustand, wechselt. ▪ No longer alarmed (Alarmzustand vorbei): Die EMX-Einheit führt die Aktion nur aus, wenn der gewählte Sensor in den Normalzustand zurückkehrt. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn der gewählte Sensor in den Alarmzustand wechselt oder diesen verlässt.
Sensorverfügbarkeit	Verfügbare Optionsfelder sind "Unavailable" (Nicht verfügbar), "Available" (Verfügbar) und "Both" (Beides). ▪ Unavailable (Nicht verfügbar): Die EMX-Einheit führt die Aktion nur aus, wenn der gewählte Sensor NICHT erkannt wird und nicht verfügbar wird. ▪ Available (Verfügbar): Die EMX-Einheit führt die Aktion nur aus, wenn der gewählte Sensor erkannt und verfügbar wird. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn der gewählte Sensor nicht verfügbar oder verfügbar wird.
Verbindungsstatus der Netzwerkschnittstelle	Verfügbare Optionsfelder sind "Link state is up" (Verbindung steht), "Link state is down" (Verbindung unterbrochen) und "Both" (Beides). ▪ Link state is up (Verbindung steht): Die EMX-Einheit führt die Aktion nur aus, wenn der Status der Netwerkverbindung von unterbrochen zu verbunden wechselt. ▪ Link state is down (Verbindung unterbrochen): Die EMX-Einheit führt die Aktion nur aus, wenn der Status der Netwerkverbindung von verbunden zu unterbrochen wechselt. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn der Status der Netwerkverbindung wechselt.

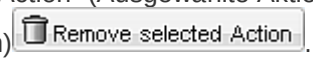
Ereignistypen	Optionsfelder
Funktion aktiviert oder deaktiviert	Verfügbare Optionsfelder sind "Enabled" (Aktiviert), "Disabled" (Deaktiviert) und "Both" (Beides). ▪ Enabled (Aktiviert): Die EMX-Einheit führt die Aktion nur aus, wenn die gewählte Funktion aktiviert ist. ▪ Disabled (Deaktiviert): Die EMX-Einheit führt die Aktion nur aus, wenn die gewählte Funktion deaktiviert ist. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn die gewählte Funktion entweder aktiviert oder deaktiviert ist.
Benutzeranmeldung oder -abmeldung	Verfügbare Optionsfelder sind "Logged in" (Angemeldet), "Logged out" (Abgemeldet) und "Both" (Beides). ▪ Logged in (Angemeldet): Die EMX-Einheit führt die Aktion nur aus, wenn sich der gewählte Benutzer anmeldet. ▪ Logged out (Abgemeldet): Die EMX-Einheit führt die Aktion nur aus, wenn sich der gewählte Benutzer abmeldet. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn sich der gewählte Benutzer an- oder abmeldet.
Serverüberwachungsereignis	Verfügbare Optionsfelder sind "Monitoring started" (Überwachung begonnen), "Monitoring stopped" (Überwachung beendet) und "Both" (Beides). ▪ Monitoring started (Überwachung begonnen): Die EMX-Einheit führt die Aktion nur aus, wenn die Überwachung eines beliebigen angegebenen Servers beginnt. ▪ Monitoring stopped (Überwachung beendet): Die EMX-Einheit führt die Aktion nur aus, wenn die Überwachung eines beliebigen angegebenen Servers endet. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn die Überwachung eines beliebigen angegebenen Servers beginnt oder endet.

Ereignistypen	Optionsfelder
Servererreichbarkeit	Verfügbare Optionsfelder sind "Unreachable" (Nicht erreichbar), "Reachable" (Erreichbar) und "Both" (Beides). ▪ Unreachable (Unerreichbar): Die EMX-Einheit führt die Aktion nur aus, wenn auf einen beliebigen angegebenen Server nicht mehr zugegriffen werden kann. ▪ Reachable (Erreichbar): Die EMX-Einheit führt die Aktion nur aus, wenn auf einen beliebigen angegebenen Server wieder zugegriffen werden kann. ▪ Both (Beides): Die EMX-Einheit führt die Aktion aus, wenn auf einen beliebigen angegebenen Server nicht mehr oder wieder zugegriffen werden kann.

1. Klicken Sie im Feld "Actions" (Aktionen) auf den Dropdown-Pfeil, wählen Sie die gewünschte Aktion aus der Liste aus, und klicken Sie auf die Schaltfläche "Add Action" (Aktion hinzufügen)

, um die Aktion hinzuzufügen.

   Die hinzugefügte Aktion wird im Listenfeld rechts neben dem Feld "Actions" (Aktionen) aufgelistet.

2. Zum Hinzufügen weiterer Aktionen wiederholen Sie Schritt 7.
3. Um eine hinzugefügte Aktion zu entfernen, wählen Sie diese im Listenfeld aus, und klicken Sie dann auf die Schaltfläche "Remove selected Action" (Ausgewählte Aktion entfernen) 

.
4. Klicken Sie auf "Save" (Speichern), um die neue Ereignisregel zu speichern.

   Hinweis: Wenn Sie nicht auf "Save" (Speichern) klicken, bevor Sie die Seite für die aktuellen Einstellungen verlassen, wird eine Meldung angezeigt. Klicken Sie anschließend auf "Yes" (Ja), um die Änderungen zu speichern, auf "Discard" (Verwerfen), um die Änderungen zu verwerfen, oder auf "Cancel" (Abbrechen), um auf die Seite mit den aktuellen Einstellungen zurückzukehren.

5. Wiederholen Sie Schritt 2 bis 10, um weitere Ereignisregeln zu erstellen.
6. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Hinweis: Ereignisregeln für Asset-Management-Sensoren müssen nach einem EMX-Firmware-Upgrade neu erstellt werden.

Erstellen von Aktionen

Die EMX-Einheit wird mit zwei integrierten Aktionen ausgeliefert:

- System Event Log Action (Systemereignisprotokoll-Aktion): Diese Aktion zeichnet das ausgewählte Ereignis bei seinem Auftreten im internen Protokoll auf.
- System SNMP Trap Action (System-SNMP-Trap-Aktion): Diese Aktion sendet SNMP-Traps an eine oder mehrere IP-Adressen, nachdem das ausgewählte Ereignis aufgetreten ist.

Hinweis: Für "System SNMP Trap Action" (System-SNMP-Trap-Aktion) werden standardmäßig keine IP-Adressen angegeben. Sie müssen daher IP-Adressen angeben, bevor diese Aktion auf eine Ereignisregel angewendet wird.

Die integrierten Aktionen können nicht gelöscht werden. Wenn diese Aktionen Ihre Anforderungen nicht erfüllen, erstellen Sie neue Aktionen.

So erstellen Sie neue Aktionen:

1. Klicken Sie auf die Registerkarte "Actions" (Aktionen).
2. Klicken Sie auf "New Action" (Neue Aktion).
3. Geben Sie in das Feld "Action name" (Aktionsname) einen Namen für die Aktion ein. Der Standardname lautet "New Action" (Neue Aktion) <Nummer>, wobei <Nummer> einer laufenden Nummer entspricht.
4. Klicken Sie im Feld "Action" (Aktion) auf den Dropdown-Pfeil, und wählen Sie die gewünschte Aktion aus der Liste aus. Die Beschreibungen finden Sie unten.
5. Klicken Sie auf "Save" (Speichern).

   Hinweis: Wenn Sie nicht auf "Save" (Speichern) klicken, bevor Sie die Seite für die aktuellen Einstellungen verlassen, wird eine Meldung angezeigt. Klicken Sie anschließend auf "Yes" (Ja), um die Änderungen zu speichern, auf "Discard" (Verwerfen), um die Änderungen zu verwerfen, oder auf "Cancel" (Abbrechen), um auf die Seite mit den aktuellen Einstellungen zurückzukehren.
6. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Option	Beschreibung
Execute an action group (Aktionsgruppe ausführen)	Bei dieser Option können Sie wählen, welche Aktion bei Auslösen eines Ereignisses ausgeführt wird. • SMS • System Event Action Log (Systemereignis-Aktionsprotokoll) • System SNMP Trap Action (System-SNMP-Trap-Aktion) *Hinweis: Um SMS-Nachrichten senden zu können, muss ein Cinterion® GSM-Modem vom Typ MC52i an die EMX-Einheit angeschlossen sein.*
"Log event message" (Protokollereignisnachricht)	Diese Option zeichnet die ausgewählten Ereignisse im internen Protokoll auf.

Option	Beschreibung
Send Snapshots via Email (Momentaufnahmen per E-Mail senden)	Mit dieser Option wird mindestens eine Person über die ausgewählten Ereignisse benachrichtigt, indem Momentaufnahmen oder Videos per E-Mail gesendet werden, die von einer angeschlossenen Logitech® QuickCam® Pro 9000-Webcam erstellt wurden (sofern vorhanden). ▪ Geben Sie im Feld "Recipients email addresses" (E-Mail-Adressen der Empfänger) die E-Mail-Adresse(n) der Empfänger an. Trennen Sie mehrere E-Mail-Adressen durch Kommata voneinander. ▪ Zur Verwendung des SMTP-Servers, der im Dialogfeld "SMTP Server Settings" (SMTP-Server-Einstellungen) angegeben ist, aktivieren Sie das Kontrollkästchen "Use Default SMTP Server" (Standard-SMTP-Server verwenden). Zur Verwendung eines anderen SMTP-Servers aktivieren Sie das Kontrollkästchen "Use Custom SMTP Settings" (Benutzerdefinierte SMTP-Einstellungen verwenden). Wenn die SMTP-Server-Einstellungen noch nicht konfiguriert sind, klicken Sie auf "Configure" (Konfigurieren). Siehe ***Konfigurieren der SMTP-Einstellungen*** (auf Seite 93), um Informationen zu den einzelnen Feldern zu erhalten. ▪ Wählen Sie die Webcam aus, die die Bilder aufnimmt, die Sie in der E-Mail senden möchten. ▪ Geben Sie im Feld "Number of Snapshots" (Anzahl Momentaufnahmen) die Anzahl der Momentaufnahmen ein, die in der bei Eintreten des Ereignisses aufgenommenen Bildfolge enthalten sein sollen. Sie können z. B. angeben, dass 10 Bilder aufgenommen werden sollen, wenn die Aktion durch das Ereignis ausgelöst wird. ▪ Geben Sie im Feld "Snapshots/Mail" (Momentaufnahmen/E-Mail) die maximale Anzahl Momentaufnahmen aus der Folge ein, die gleichzeitig in der E-Mail gesendet werden sollen. ▪ Geben Sie im Feld "Time before first Snapshot (s):" (Zeit vor erster/n Momentaufnahme(n):) die Zeit in Sekunden ein, die zwischen dem Auslösen des Ereignisses und der Aufzeichnung von Momentaufnahmen verstreichen soll. ▪ Geben Sie im Feld "Time between Snapshots (s):" (Zeit zwischen Momentaufnahme (s):) die Zeit an, die zwischen den einzelnen Momentaufnahmen verstreichen soll.

Option	Beschreibung
Send EMail (E-Mail senden)	Diese Aktion sendet eine E-Mail an angegebene Empfänger, um sie über das Eintreten des Ereignisses zu benachrichtigen. • Geben Sie im Feld "Recipients email addresses" (E-Mail-Adressen der Empfänger) die E-Mail-Adresse(n) der Empfänger an. Trennen Sie mehrere E-Mail-Adressen durch Kommata voneinander. • Zur Verwendung des SMTP-Servers, der im Dialogfeld "SMTP Server Settings" (SMTP-Server-Einstellungen) angegeben ist, aktivieren Sie das Kontrollkästchen "Use Default SMTP Server" (Standard-SMTP-Server verwenden). Zur Verwendung eines anderen SMTP-Servers aktivieren Sie das Kontrollkästchen "Use Custom SMTP Settings" (Benutzerdefinierte SMTP-Einstellungen verwenden). Wenn die SMTP-Server-Einstellungen noch nicht konfiguriert sind, klicken Sie auf "Configure" (Konfigurieren). Siehe ***Konfigurieren der SMTP-Einstellungen*** (auf Seite 93), um Informationen zu den einzelnen Feldern zu erhalten. Standardnachrichten werden auf Basis des Ereignisses gesendet. Eine Liste der Standard-Protokollnachrichten und Ereignisse, die sie auslösen, finden Sie unter ***Standard-Protokollnachrichten*** (auf Seite 151). • Aktivieren Sie bei Bedarf das Kontrollkästchen "Use Custom Log Message" (Benutzerdefinierte Protokollnachricht verwenden), und geben Sie eine benutzerdefinierte Nachricht in das bereitgestellte Feld ein. Siehe ***Erstellen von benutzerdefinierten E-Mail-Nachrichten*** (auf Seite 149).

Option	Beschreibung
"Send SNMP trap" (SNMP-Trap senden)	Diese Option sendet SNMP-Traps an einen oder mehrere SNMP-Manager. • Sie können bis zu 3 SNMP-Trap-Ziele in den Feldern für "Host *x*" angeben, wobei *x* eine Zahl zwischen 1 und 3 ist. • Geben Sie eine Port-Nummer für jedes Ziel in die Felder für "Port *x*" ein, wobei *x* eine Zahl zwischen 1 und 3 ist. • Geben Sie einen Community-String für jedes Ziel in die Felder für "Community *x*" ein, wobei *x* eine Zahl zwischen 1 und 3 ist.
Syslog message (Syslog-Nachricht)	Diese Option sorgt dafür, dass die EMX-Einheit Ereignismeldungen automatisch an den angegebenen Syslog-Server weiterleitet. ▪ Geben Sie im Feld "Syslog server" (Syslog-Server) die IP-Adresse ein, an die das Syslog weitergeleitet werden soll. ▪ Geben Sie im Feld "Port" eine entsprechende Port-Nummer ein.
Send SMS message (SMS-Nachricht senden)	Sendet eine Textnachricht an das angegebene Handy. Um SMS-Nachrichten senden zu können, muss ein Cinterion® GSM-Modem vom Typ MC52i an die EMX-Einheit angeschlossen sein. *Hinweis: Die EMX-Einheit kann keine SMS-Nachrichten empfangen.* *Hinweis: Bei SMS-Nachrichten wird nur Englisch unterstützt.* • Geben Sie die Telefonnummer in das Feld "Recipient's Phone Number" (Telefonnummer des Empfängers) ein.

Option	Beschreibung
Record Snapshots to Webcam Storage (Momentaufnahmen in Webcam-Speicher aufzeichnen)	Mit dieser Option können Sie eine Aktion definieren, durch die eine bestimmte Webcam die Aufzeichnung von Momentaufnahmen beginnt oder beendet. ▪ Geben Sie die Gesamtanzahl der Momentaufnahmen ein, die bei Eintreten des Ereignisses aufgezeichnet werden sollen. Auf der EMX-Einheit können maximal zehn (10) Momentaufnahmen gespeichert werden. Wenn Sie einen Wert größer als zehn eingeben, werden die Momentaufnahmen nach der zehnten aufgenommenen und gespeicherten Aufnahme überschrieben. ▪ Geben Sie im Feld "Time before first Snapshot (s):" (Zeit vor erster/n Momentaufnahme(n):) die Zeit in Sekunden ein, die zwischen dem Auslösen des Ereignisses und der Aufzeichnung von Momentaufnahmen verstreichen soll. ▪ Geben Sie im Feld "Time between Snapshots (s):" (Zeit zwischen Momentaufnahme (s):) die Zeit an, die zwischen den einzelnen Momentaufnahmen verstreichen soll.

Erstellen von benutzerdefinierten E-Mail-Nachrichten

Sie können einer in einer E-Mail enthaltene Nachricht anpassen, wenn Sie E-Mails konfiguriert haben, die bei Eintreten eines Ereignisses gesendet werden sollen.

Nachrichten bestehen aus einer Kombination von Text und EMX-Platzhaltern. Die Platzhalter stehen für Informationen, die von der EMX-Einheit extrahiert und in die Nachricht eingefügt werden.

Beispiel:

```
[USERNAME] logged into the device on [TIMESTAMP]
([BENUTZERNAME] hat sich am [TIMESTAMP] beim Gerät
angemeldet
```

wird zu

```
JQPublic logged into the device on 2012-January-30 21:00
(JQPublic hat sich am 30. Januar 2012 um 21:00 beim Gerät
angemeldet)
```

Eine Liste und eine Definition der verschiedenen Variablen finden Sie unter ***Platzhalter in E-Mail-Nachrichten*** (auf Seite 150).

So erstellen Sie eine benutzerdefinierte Nachricht:

1. Klicken Sie auf "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln).
2. Klicken Sie auf die Registerkarte "Actions" (Aktionen).
3. Wählen Sie im linken Fensterbereich das Ereignis aus, mit dem die Aktion verknüpft ist, oder erstellen Sie eine neue Aktion. Siehe ***Erstellen von Aktionen*** (auf Seite 143).
4. Wählen Sie "Send EMail" (E-Mail senden) aus der Dropdown-Liste "Actions" (Aktionen) im Bereich "Action Settings" (Aktionseinstellungen) des Dialogfelds.
5. Aktivieren Sie das Kontrollkästchen "Use Custom Log Message" (Benutzerdefinierte Protokollnachricht verwenden).
6. Erstellen Sie die Nachricht im angezeigten Textfeld, indem Sie benutzerdefinierte Informationen eingeben. Setzen Sie bei Bedarf Platzhalter in die Nachricht ein.

   Hinweis: Klicken Sie auf das Informationssymbol , um das Dialogfeld "Event Context Information" (Ereigniskontextinformationen) zu öffnen, das eine Liste mit Platzhaltern und der zugehörigen Definition enthält.

7. Klicken Sie auf "Save" (Speichern).

Platzhalter in E-Mail-Nachrichten

Im Folgenden sind die Platzhalter aufgeführt, die in benutzerdefinierten E-Mail-Nachrichten für Ereignisse verwendet werden können.

Hinweis: Klicken Sie auf das Informationssymbol , um das Dialogfeld "Event Context Information" (Ereigniskontextinformationen) zu öffnen, das eine Liste mit Platzhaltern und der zugehörigen Definition enthält.

Platzhalter	Beschreibung
[ASSERTION]	Boolesches Flag, wenn eine Ereignisbedingung eintrat (1) oder beendet wurde (0)
[EXTSENSORNAME]	Der Name eines externen Sensors
[EXTSENSORSLOT]	Die ID für den Slot eines externen Sensors
[IFNAME]	Der Name einer Netzwerkschnittstelle in einer für den Menschen lesbaren Form
[VALUE]	Der neue Wert eines Parameters
[VERSION]	Die Firmware-Version, auf die das Gerät aktualisiert wird
[OLDVERSION]	Die Firmware-Version, von der das Gerät aktualisiert wird
[PARAMETER]	Der Name eines Konfigurationsparameters
[PORTID]	Die Kennzeichnung des externen Ports, an den das Gerät angeschlossen ist, das das Ereignis ausgelöst hat
[PORTTYPE]	Der Typ des externen Ports, z. B. 'feature' (Feature) oder 'auxiliary' (Zusatz), an den das Gerät angeschlossen ist, das das Ereignis ausgelöst hat
[RECIPIENTS]	Die Liste der Empfänger, an die eine SMTP-Nachricht gesendet wurde
[TARGETROLE]	Der Name der Benutzerverwaltungsfunktion, auf die eine Aktion angewendet wurde
[SERVER]	Der Name oder die IP-Adresse eines Servers
[TARGETUSER]	Der Benutzer, für den eine Aktion ausgelöst wurde
[TIMESTAMP]	Die Zeitmarke für den Eintritt des Ereignisses
[USERIP]	Die IP-Adresse, über die ein Benutzer eine Verbindung hergestellt hat
[USERNAME]	Der Benutzer, der eine Aktion ausgelöst hat

[LEDCOLOR]	Die RGB-LED-Farbe
[LEDMODE]	Der LED-Anzeigemodus
[LEDOPMODE]	Der LED-Betriebsmodus
[STATE]	Der Zustand eines Assetstrips in einer für den Menschen lesbaren Form
[RACKUNIT]	Die (vertikale) Position der Rackeinheit, auf die sich eine Aktion bezieht
[RACKSLOT]	Die (horizontale) Slot-Position, auf die sich eine Aktion bezieht
[STRIPNAME]	Der Name eines Assetstrips
[STRIPID]	Die numerische ID eines Assetstrips
[TAGID]	Die Asset-Tag-ID
[LDAPERRORDESC]	Ein LDAP-Fehler ist aufgetreten
[LHXFANID]	Die ID eines Lüfters, der an einen LHX angeschlossen ist
[LHXPOWERSUPPLYID]	Die ID einer LHX-Stromversorgungseinheit
[LHXSENSORID]	Die ID eines LHX-Sensors
[INLETPOLE]	Die ID der Eingangsstromleitung
[INLETSENSOR]	Der Name des Eingangssensors
[INLET]	Die Bezeichnung des Stromeingangs
[OCPSENSOR]	Der Name des Überstromschutzsensors
[OCP]	Die Bezeichnung des Überstromschutzes
[OUTLETPOLE]	Die ID der Ausgangsstromleitung
[OUTLETSENSOR]	Der Name des Ausgangssensors
[OUTLET]	Die Bezeichnung des Ausgangs
[POLESENSOR]	Der Sensorname für eine bestimmte Stromleitung

Standard-Protokollnachrichten

Im Folgenden sind Standard-Protokollnachrichten aufgeführt, die ausgelöst und an angegebene Empfänger gesendet werden, wenn EMX-Ereignisse eintreten (TRUE sind) oder, in manchen Fällen, nicht eintreten (FALSE sind). Informationen zum Konfigurieren von E-Mail-Nachrichten, die bei Eintreten angegebener Ereignisse gesendet werden sollen, finden Sie unter ***Ereignisregeln und Aktionen*** (auf Seite 137).

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
Gerät > System gestartet	System started. (System gestartet.)	
Gerät > System zurückgesetzt	System reset performed by user '[USERNAME]' from host '[USERIP]'. (System durch Benutzer '[USERNAME]' von Host '[USERIP]' zurückgesetzt).	
Gerät > Firmware-Validierung fehlgeschlagen	System reset performed by user '[USERNAME]' from host '[USERIP]'. (System durch Benutzer '[USERNAME]' von Host '[USERIP]' zurückgesetzt).	
Gerät > Firmware-Aktualisierung gestartet	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Firmware-Aktualisierung von Version '[OLDVERSION]' auf Version '[VERSION]' durch Benutzer '[USERNAME]' von Host '[USERIP]' gestartet.)	
Gerät > Firmware-Aktualisierung beendet	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Firmware-Aktualisierung von Version '[OLDVERSION]' auf Version '[VERSION]' durch Benutzer '[USERNAME]' von Host '[USERIP]' erfolgreich ausgeführt.)	
Gerät > Firmware-Aktualisierung fehlgeschlagen	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (Firmware-Aktualisierung von Version '[OLDVERSION]' auf Version '[VERSION]' durch Benutzer '[USERNAME]' von Host '[USERIP]' fehlgeschlagen.)	
Gerät > Geräte-ID geändert	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'. (Konfigurationsparameter '[PARAMETER]' durch Benutzer '[USERNAME]' von Host '[USERIP]' in	

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
	'[VALUE]' geändert.)	
Gerät > Ereignisprotokoll gelöscht	Event log cleared by user '[USERNAME]' from host '[USERIP]'. (Ereignisprotokoll durch Benutzer '[USERNAME]' von Host '[USERIP]' gelöscht.)	
Gerät > Sammelkonfiguration gespeichert	Bulk configuration saved from host '[USERIP]'. (Sammelkonfiguration von Host '[USERIP]' gespeichert.)	
Gerät > Sammelkonfiguration kopiert	Bulk configuration copied from host '[USERIP]'. (Sammelkonfiguration von Host '[USERIP]' kopiert.)	
Gerät > Verbindung der Netzwerkschnittstelle steht	The [IFNAME] network interface link is now up. (Die Verbindung der Netzwerkschnittstelle [IFNAME] steht jetzt.)	The [IFNAME] network interface link is now down. (Die Verbindung der Netzwerkschnittstelle [IFNAME] ist jetzt unterbrochen.)
Gerät > Senden von SMTP-Meldung fehlgeschlagen	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed. (Senden von SMTP-Meldung an '[RECIPIENTS]' mit Server '[SERVER]' fehlgeschlagen.)	
Gerät > LDAP-Fehler	An LDAP error occured: [LDAPERRORDESC]. (Ein LDAP-Fehler ist aufgetreten: [LDAPERRORDESC].)	
Gerät > USB-Slave angeschlossen	USB slave connected. (USB-Slave angeschlossen.)	USB slave disconnected. (USB-Slave nicht angeschlossen.)
Gerät > Funktionen > Schroff LHX-Unterstützung	Schroff LHX support enabled. (Schroff LHX-Unterstützung aktiviert.)	Schroff LHX support disabled. (Schroff LHX-Unterstützung deaktiviert.)
Benutzerverwaltung > Benutzer hinzugefügt	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'. (Benutzer '[TARGETUSER]' durch Benutzer '[USERNAME]' von Host '[USERIP]' hinzugefügt.)	
Benutzerverwaltung > Benutzer geändert	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'. (Benutzer '[TARGETUSER]' durch Benutzer '[USERNAME]' von Host '[USERIP]' geändert.)	
Benutzerverwaltung > Benutzer	User '[TARGETUSER]' deleted by user	

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
gelöscht	'[USERNAME]' from host '[USERIP]'. (Benutzer '[TARGETUSER]' durch Benutzer '[USERNAME]' von Host '[USERIP]' gelöscht.)	
Benutzerverwaltung > Kennwort geändert	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'. (Kennwort des Benutzers '[TARGETUSER]' durch Benutzer '[USERNAME]' von Host '[USERIP]' geändert.)	
Benutzerverwaltung > Kennworteinstellungen geändert	Password settings changed by user '[USERNAME]' from host '[USERIP]'. (Kennworteinstellungen durch Benutzer '[USERNAME]' von Host '[USERIP]' geändert.)	
Benutzerverwaltung > Benutzerfunktion hinzugefügt	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'. (Benutzerfunktion '[TARGETROLE]' durch Benutzer '[USERNAME]' von Host '[USERIP]' hinzugefügt.)	
Benutzerverwaltung > Benutzerfunktion geändert	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'. (Benutzerfunktion '[TARGETROLE]' durch Benutzer '[USERNAME]' von Host '[USERIP]' geändert.)	
Benutzerverwaltung > Benutzerfunktion gelöscht	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'. (Benutzerfunktion '[TARGETROLE]' durch Benutzer '[USERNAME]' von Host '[USERIP]' gelöscht.)	
Benutzeraktivität > * > Benutzer angemeldet	User '[USERNAME]' from host '[USERIP]' logged in. (Benutzer '[USERNAME]' von Host '[USERIP]' angemeldet.)	User '[USERNAME]' from host '[USERIP]' logged out. (Benutzer '[USERNAME]' von Host '[USERIP]' abgemeldet.)
Benutzeraktivität > * > Authentifizierungsfehler	Authentication failed for user '[USERNAME]' from host '[USERIP]'. (Authentifizierung für Benutzer '[USERNAME]' von Host '[USERIP]' fehlgeschlagen).	
Benutzeraktivität > * > Benutzer gesperrt	User '[USERNAME]' from host '[USERIP]' was blocked. (Benutzer '[USERNAME]' von Host '[USERIP]'	

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
	wurde gesperrt.)	
Benutzeraktivität > * > Zeitüberschreitung bei Sitzung	Session of user '[USERNAME]' from host '[USERIP]' timed out. (Sitzung des Benutzers '[USERNAME]' von Host '[USERIP]' überschritt Zeitlimit.)	
Überstromschutz > * > Sensor > * > Nicht verfügbar	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable. (Sensor '[OCPSENSOR]' an Überstromschutz '[OCP]' nicht verfügbar.)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available. (Sensor '[OCPSENSOR]' an Überstromschutz '[OCP]' verfügbar.)
Slot des externen Sensors > * > Numerischer Sensor > Nicht verfügbar	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' nicht verfügbar.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' verfügbar.)
Slot des externen Sensors > * > Numerischer Sensor > Über oberem kritischen Schwellenwert	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Assertion 'über oberem kritischen Schwellenwert' durch.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Deassertion 'über oberem kritischen Schwellenwert' durch.)
Slot des externen Sensors > * > Numerischer Sensor > Über oberem Warnschwellenwert	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Assertion 'über oberem Warnschwellenwert' durch.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Deassertion 'über oberem Warnschwellenwert' durch.)
Slot des externen Sensors > * > Numerischer Sensor > Unter unterem Warnschwellenwert	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Assertion 'unter unterem Warnschwellenwert' durch.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning'. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Deassertion 'unter unterem Warnschwellenwert' durch.)
Slot des externen Sensors > * > Numerischer Sensor > Unter unterem kritischen	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'. (Externer Sensor '[EXTSENSORNAME]' in Slot	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'. (Externer

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
Schwellenwert	'[EXTSENSORSLOT]' führte Assertion 'unter unterem kritischen Schwellenwert' durch.)	Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' führte Deassertion 'unter unterem kritischen Schwellenwert' durch.)
Slot des externen Sensors > * > Status Sensor > Nicht verfügbar	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' nicht verfügbar.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' verfügbar.)
Slot des externen Sensors > * > Status Sensor > Geschlossen	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' geschlossen.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is open. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' offen.)
Slot des externen Sensors > * > Status Sensor > Ein	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' eingeschaltet.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is off. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' ausgeschaltet.)
Slot des externen Sensors > * > Status Sensor > Alarm	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' im Alarmzustand.)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed. (Externer Sensor '[EXTSENSORNAME]' in Slot '[EXTSENSORSLOT]' nicht mehr im Alarmzustand.)
Serverüberwachung > * > Überwacht	Server '[SERVER]' is now being monitored. (Server '[SERVER]' wird jetzt überwacht.)	Server '[SERVER]' is no longer being monitored. (Server '[SERVER]' wird nicht mehr überwacht.)
Serverüberwachung > * > Nicht erreichbar	Server '[SERVER]' is unreachable. (Server '[SERVER]' ist nicht erreichbar.)	Server '[SERVER]' is reachable. (Server '[SERVER]' ist erreichbar.)
Asset-Management > Status	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (Status des Assetstrips [STRIPID] ('[STRIPNAME]') in '[STATE]' geändert.)	

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
Asset-Management > Rackeinheit > * > Tag angeschlossen	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (Asset-Tag mit ID '[TAGID]' an Rackeinheit [RACKUNIT], Slot [RACKSLOT] des Assetstrips [STRIPID] ('[STRIPNAME]') angeschlossen.)	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (Asset-Tag mit ID '[TAGID]' nicht an Rackeinheit [RACKUNIT], Slot [RACKSLOT] des Assetstrips [STRIPID] ('[STRIPNAME]') angeschlossen.)
Asset-Management > Rackeinheit > * > Blade-Erweiterung angeschlossen	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (Blade-Erweiterung mit ID '[TAGID]' an Rackeinheit [RACKUNIT] des Assetstrips [STRIPID] ('[STRIPNAME]') angeschlossen.)	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (Blade-Erweiterung mit ID '[TAGID]' an Rackeinheit [RACKUNIT] des Assetstrips [STRIPID] ('[STRIPNAME]') nicht angeschlossen.)
Asset-Management > Firmware-Aktualisierung	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'. (Firmware-Aktualisierung für Assetstrip [STRIPID] ('[STRIPNAME]'): Status in '[STATE]' geändert.)	
Asset-Management > Gerätekonfiguration geändert	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'. (Konfigurationsparameter '[PARAMETER]' des Assetstrips [STRIPID] ('[STRIPNAME]') von Benutzer '[USERNAME]' in '[VALUE]' geändert.)	
Asset-Management > Rackeinheitenkonfiguration geändert	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]' (Konfiguration der Rackeinheit [RACKUNIT] des Assetstrips [STRIPID] ('[STRIPNAME]') von Benutzer '[USERNAME]' geändert in: LED-Betriebsmodus '[LEDOPMODE]', LED-Farbe '[LEDCOLOR]', LED-Modus '[LEDMODE]')	

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
Asset-Management > Überlauf Blade-Erweiterung	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]'). (Überlauf der Blade-Erweiterung bei Strip [STRIPID] ('[STRIPNAME]') aufgetreten.)	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]'). (Überlauf der Blade-Erweiterung für Strip [STRIPID] ('[STRIPNAME]') beseitigt.)
Asset-Management > Zusammensetzung des Komposit-Assetstrips geändert	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]'). (Zusammensetzung des Komposit-Assetstrips [STRIPID] ('[STRIPNAME]') geändert.)	
**LHX > Angeschlossen	LHX has been connected to [PORTTYPE] port [PORTID]. (LHX wurde an [PORTTYPE] Port [PORTID] angeschlossen.)	LHX has been disconnected from [PORTTYPE] port [PORTID]. (LHX wurde von [PORTTYPE] Port [PORTID] getrennt.)
**LHX > Betriebszustand	LHX connected to [PORTTYPE] port [PORTID] has been switched on. (An [PORTTYPE] Port [PORTID] angeschlossener LHX wurde eingeschaltet.)	LHX connected to [PORTTYPE] port [PORTID] has been switched off (An [PORTTYPE] Port [PORTID] angeschlossener LHX wurde ausgeschaltet.)
**LHX > Sensor > Nicht verfügbar	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' nicht verfügbar.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' verfügbar.)
**LHX > Sensor > Über oberem kritischen Schwellenwert	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Assertion 'über oberem kritischen Schwellenwert' durch.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Deassertion 'über oberem kritischen Schwellenwert' durch.)
**LHX > Sensor > Über oberem Warnschwellenwert	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Assertion 'über oberem Warnschwellenwert' durch.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Deassertion 'über oberem Warnschwellenwert' durch.)
**LHX > Sensor > Unter	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]'

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
unterem Warnschwellenwert	'below lower warning'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Assertion 'unter unterem Warnschwellenwert' durch.)	deasserted 'below lower warning'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Deassertion 'unter unterem Warnschwellenwert' durch.)
**LHX > Sensor > Unter unterem kritischen Schwellenwert	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Assertion 'unter unterem kritischen Schwellenwert' durch.)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'. (Sensor '[LHXSENSORID]' auf LHX an [PORTTYPE] Port '[PORTID]' führte Deassertion 'unter unterem kritischen Schwellenwert' durch.)
**LHX > Notkühlung	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated. (Notkühlung auf LHX an [PORTTYPE] Port '[PORTID]' wurde aktiviert.)	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated. (Notkühlung auf LHX an [PORTTYPE] Port '[PORTID]' wurde deaktiviert.)
**LHX > Anforderung maximale Kühlung	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'. (Für LHX an [PORTTYPE] Port '[PORTID]' wurde maximale Kühlung angefordert.)	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'. (Für LHX an [PORTTYPE] Port '[PORTID]' wird keine maximale Kühlung mehr angefordert.)
**LHX > Parameterdatenverlust	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'. (Datenverlust in Parameterspeicher auf LHX an [PORTTYPE] Port '[PORTID]' festgestellt.)	
**LHX > ST-Bus-Kommunikationsfehler	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'. (ST-Bus-Kommunikationsfehler auf LHX an [PORTTYPE] Port '[PORTID]' festgestellt.)	
**LHX > Sammelfehler	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' ist ein Sammelfehler aufgetreten.)	
**LHX > Türkontakt	The door of LHX at [PORTTYPE] port '[PORTID]' was opened. (Die Tür des LHX an [PORTTYPE] Port '[PORTID]'	The door of LHX at [PORTTYPE] port '[PORTID]' was closed. (Die Tür des LHX an [PORTTYPE] Port '[PORTID]' wurde

Ereignis/Kontext	Standard-Assertionsmeldung, wenn Ereignis = TRUE	Standard-Assertionsmeldung, wenn Ereignis = FALSE*
	wurde geöffnet.)	geschlossen.)
**LHX > Sensorfehler	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' bei Sensor '[LHXSENSORID]' ist ein Sensorfehler (unterbrochener Stromkreis oder Kurzschluss) aufgetreten).	
**LHX > Lüfterfehler	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' bei Lüfter '[LHXFANID]' ist ein Lüftermotorfehler aufgetreten.)	
**LHX > Stromversorgungsfehler	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' bei Stromversorgungseinheit '[LHXPOWERSUPPLYID]' ist ein Stromversorgungsfehler aufgetreten.)	
**LHX > Feuchtigkeitsschwellenwert	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (Der Feuchtigkeitsschwellenwert auf LHX an [PORTTYPE] Port '[PORTID]' wurde über-/unterschritten.)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (Die Feuchtigkeit auf LHX an [PORTTYPE] Port '[PORTID]' liegt innerhalb der Schwellenwerte.)
**LHX > Fehler externe Wasserkühlung	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' ist bei der externen Wasserkühlung ein Fehler aufgetreten.)	
**LHX > Wasserleck	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'. (Auf LHX an [PORTTYPE] Port '[PORTID]' wurde ein Wasserleck festgestellt.)	

**Hinweis: Nicht für Auslösungsereignisse festgelegt (siehe [ASSERTION] ctx)*

***Hinweis: LHX-Ereignisse sind nur verfügbar, wenn die Schroff LHX-Unterstützung aktiviert ist.*

Beispiel-Ereignisregeln

Beispiel-Ereignisregel auf Asset-Management-Ebene

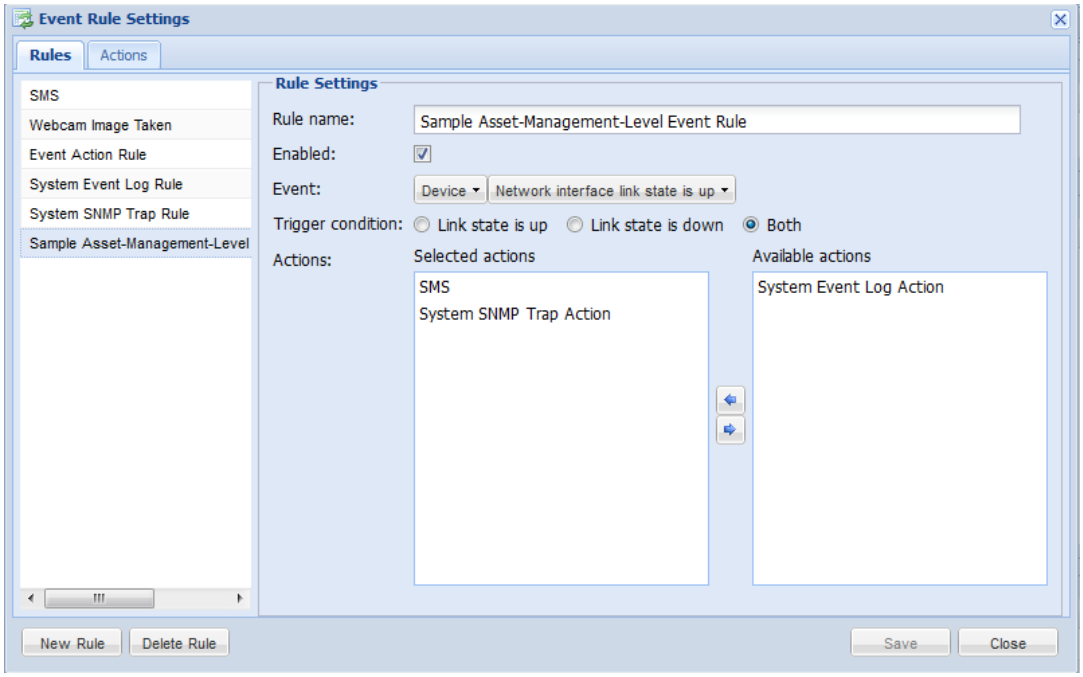
In diesem Beispiel soll die EMX-Einheit Einträge im internen Protokoll vornehmen, wenn die Netzwerkverbindung eines Assetsensors hergestellt oder unterbrochen wird. Die Beispiel-Ereignisregel sieht wie folgt aus:

- Event (Ereignis): Device > Network interface link state is up (Gerät > Verbindung der Netzwerkschnittstelle steht)
- Trigger condition (Auslösebedingung): Both (Beide)
- Actions (Aktionen): System Event Log Action (Systemereignisprotokoll-Aktion)

So erstellen Sie die obige Ereignisregel:

1. Geben Sie einen Namen für die Regel ein.
2. Klicken Sie auf das Kontrollkästchen "Enabled" (Aktiviert), um die Regel zu aktivieren.
3. Wählen Sie in der Dropdown-Liste "Event" (Ereignis) den Eintrag "Device" > "Network interface link state is up" (Gerät > Verbindung der Netzwerkschnittstelle steht). Diese Auswahl bedeutet, dass wir ein Ereignis hinsichtlich der Assetsensorverwaltung angeben und dass die EMX-Einheit auf das Ereignis reagieren soll, bei dem eine physische Verbindung hergestellt oder unterbrochen wird.
4. Wählen Sie die Option "Both" (Beide), weil Verbindungs- und Trennaktionen aufgezeichnet werden sollen, wenn eine der Aktionen ausgeführt wird.

5. Wählen Sie "System Event Log Action" (Systemereignisprotokoll-Aktion), weil dieses Ereignis im internen Protokoll aufgezeichnet werden soll, wenn die angegebenen Ereignisse eintreten.



Beispiel-Ereignisregel auf Sensorebene

In diesem Beispiel soll das EMX-Gerät SNMP-Traps an den SNMP-Manager senden, wenn das Ergebnis des Temperatursensors, der an Sensor-Port 1 angeschlossen ist, einen Schwellenwert über- oder unterschreitet, oder wenn der Sensor nicht verfügbar ist. Um dies zu erreichen, muss eine Ereignisregel wie nachfolgend beschrieben erstellt werden:

- Event (Ereignis): External sensor slot (Slot des externen Sensors) > Slot 1 > Numeric Sensor (Numerischer Sensor) > Any sub-event (Beliebiges Unterereignis)
- Actions (Aktionen): System SNMP Trap Action (System-SNMP-Trap-Aktion)

So erstellen Sie die obige Ereignisregel:

1. Wählen Sie im Feld "Event" (Ereignis) die Option "External sensor slot" (Slot des externen Sensors), um anzugeben, dass ein Ereignis auf Umgebungssensor-Ebene angegeben wird.
2. Wählen Sie "Slot 1" aus dem Untermenü, weil der Bericht Informationen über den an Sensor-Port 1 angeschlossenen Sensor enthalten soll.

3. Wählen Sie "Numeric Sensor" (Numerischer Sensor), um anzugeben, dass der Sensor ein numerischer Sensor ist.

   Hinweis: Ein numerischer Sensor zeigt die Umgebungsbedingung mit numerischen Werten an, während ein Einzelsensor (Ein/Aus-Sensor) den Sensorstatus mit Buchstaben anzeigt.

4. Wählen Sie "<Any sub-event>" (Beliebiges Unterereignis), weil alle Ereignisse zu dem Sensor angegeben werden sollen, der an Sensor-Port 1 angeschlossen ist. Dazu gehören der Status "unavailable" (nicht verfügbar) sowie Schwellenwertunterschreitungen oder -überschreitungen – "Above upper critical" (Über oberem kritischen Schwellenwert), "Above upper warning" (Über oberem Warnschwellenwert), "Below lower warning" (Unter unterem Warnschwellenwert) und "Below lower critical" (Unter unterem kritischen Schwellenwert).
5. Wählen Sie "System SNMP Trap Action" (System-SNMP-Trap-Aktion), weil SNMP-Traps gesendet werden sollen, um auf die angegebenen Ereignisse zu reagieren, wenn diese Ereignisse eintreten.

Beispiel-Ereignisregel auf Benutzeraktivitätsebene

In diesem Beispiel soll das EMX-Gerät die Benutzeraktivität im internen Protokoll aufzeichnen, wenn sich ein Benutzer an- oder abmeldet. Die Ereignisregel wird wie folgt eingerichtet:

- Event (Ereignis): User activity (Benutzeraktivität) > Any user (Beliebiger Benutzer) > User logged in (Benutzer angemeldet)
- Trigger condition (Auslösebedingung): Both (Beide)
- Actions (Aktionen): System Event Log Action (Systemereignisprotokoll-Aktion)

So erstellen Sie die obige Ereignisregel:

1. Wählen Sie im Feld "Event" (Ereignis) die Option "User activity" (Benutzeraktivität), um anzugeben, dass ein Ereignis definiert wird, das die Benutzeraktivität betrifft.
2. Wählen Sie "<Any user>" (Beliebiger Benutzer) aus dem Untermenü, weil die Aktivität aller Benutzer aufgezeichnet werden soll.
3. Wählen Sie "User logged in" (Benutzer angemeldet), um Ereignisse auszuwählen, die die Benutzeranmeldung betreffen.
4. Wählen Sie die Option "Both" (Beide), weil An- und Abmeldeaktionen aufgezeichnet werden sollen, wenn eines der Ereignisse eintritt.
5. Wählen Sie "System Event Log Action" (Systemereignisprotokoll-Aktion), weil dieses Ereignis im internen Protokoll aufgezeichnet werden soll, wenn die angegebenen Ereignisse eintreten.

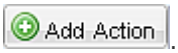
Ändern einer Ereignisregel

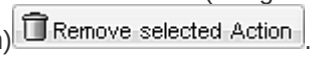
Sie können das Ereignis, die Aktion, die Auslösebedingung und andere Einstellungen einer Ereignisregel ändern.

Ausnahme: Ereignisse und Aktionen, die in den integrierten Ereignisregeln ausgewählt sind, können nicht geändert werden, einschließlich "System Event Log Rule" (Systemereignisprotokoll-Regel) und "System SNMP Trap Rule" (System-SNMP-Trap-Regel).

So ändern Sie eine Ereignisregel:

1. Wählen Sie "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln) aus. Das Fenster "Event Rule Settings" (Ereignisregeleinstellungen) wird eingeblendet.
2. Wählen Sie auf der Registerkarte "Rules" (Regeln) die Ereignisregel aus, die Sie im linken Fenster ändern möchten.
3. Zum Deaktivieren dieser Ereignisregel deaktivieren Sie das Kontrollkästchen "Enabled" (Aktiviert).
4. Zum Ändern des Ereignisses klicken Sie auf die gewünschte Registerkarte im Feld "Event" (Ereignis) und wählen ein anderes Element aus dem Pulldown-Menü oder Untermenü aus.

   Für eine Ereignisregel zur Benutzeraktivität für den Benutzer "admin" können Sie beispielsweise auf die Registerkarte "admin" klicken, um ein Pulldown-Untermenü anzuzeigen, das alle Benutzernamen anzeigt, und anschließend einen anderen Benutzernamen oder alle Benutzernamen auswählen (<*Any user*> (Beliebiger Benutzer) genannt).
5. Wenn Optionsfelder zur Verfügung stehen, können Sie ein anderes als das aktuell ausgewählte Optionsfeld auswählen, um die Auslösebedingung für die Regel zu ändern.
6. Zum Ändern der Aktion(en) führen Sie für das Feld "Actions" (Aktionen) die folgenden Schritte aus:
   - Zum Hinzufügen einer neuen Aktion klicken Sie auf den Dropdown-Pfeil, wählen die Aktion aus der Liste aus und klicken auf die Schaltfläche "Add Action" (Aktion hinzufügen) 

.
   - Um eine hinzugefügte Aktion zu entfernen, wählen Sie diese im Listenfeld aus, und klicken Sie dann auf die Schaltfläche "Remove selected Action" (Ausgewählte Aktion entfernen) 

.
7. Klicken Sie auf "Save" (Speichern), um die Änderungen zu speichern.

Hinweis: Wenn Sie nicht auf "Save" (Speichern) klicken, bevor Sie die Seite für die aktuellen Einstellungen verlassen, wird eine Meldung angezeigt. Klicken Sie anschließend auf "Yes" (Ja), um die Änderungen zu speichern, auf "Discard" (Verwerfen), um die Änderungen zu verwerfen, oder auf "Cancel" (Abbrechen), um auf die Seite mit den aktuellen Einstellungen zurückzukehren.

8. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Ändern einer Aktion

Eine vorhandene Aktion kann geändert werden, sodass alle Ereignisregeln für diese Aktion ihr Verhalten entsprechend ändern.

Ausnahme: Die integrierte Aktion "System Event Log Action" (Systemereignisprotokoll-Aktion) kann vom Benutzer nicht konfiguriert werden.

So ändern Sie eine Aktion:

1. Wählen Sie "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln) aus. Das Fenster "Event Rule Settings" (Ereignisregeleinstellungen) wird eingeblendet.
2. Klicken Sie auf die Registerkarte "Actions" (Aktionen).
3. Wählen Sie die zu ändernde Aktion aus der linken Liste aus.
4. Nehmen Sie an den angezeigten Informationen die erforderlichen Änderungen vor.
5. Klicken Sie auf "Save" (Speichern), um die Änderungen zu speichern.

Hinweis: Wenn Sie nicht auf "Save" (Speichern) klicken, bevor Sie die Seite für die aktuellen Einstellungen verlassen, wird eine Meldung angezeigt. Klicken Sie anschließend auf "Yes" (Ja), um die Änderungen zu speichern, auf "Discard" (Verwerfen), um die Änderungen zu verwerfen, oder auf "Cancel" (Abbrechen), um auf die Seite mit den aktuellen Einstellungen zurückzukehren.

6. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Löschen einer Ereignisregel oder Aktion

Wenn eine Ereignisregel oder Aktion veraltet ist, entfernen Sie sie.

Hinweis: Sie können die integrierten Ereignisregeln und Aktionen nicht löschen.

So löschen Sie eine Ereignisregel oder eine Aktion:

1. Wählen Sie "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln) aus. Das Fenster "Event Rule Settings" (Ereignisregeleinstellungen) wird eingeblendet.
2. So löschen Sie eine Ereignisregel:
   a. Stellen Sie sicher, dass die Registerkarte "Rules" (Regeln) ausgewählt ist. Falls nicht, klicken Sie auf die Registerkarte "Rules" (Regeln).
   b. Wählen Sie die gewünschte Regel aus der Liste links aus, und klicken Sie auf "Delete Rule" (Regel löschen).
   c. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
3. So löschen Sie eine Aktion:
   a. Klicken Sie auf die Registerkarte "Actions" (Aktionen).
   b. Wählen Sie die gewünschte Aktion aus der Liste links aus, und klicken Sie auf "Delete Action" (Aktion löschen).
   c. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
4. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Hinweis zu nicht ausgelösten Regeln

In einigen Fällen wird ein Schwellenwert überschritten und von der EMX-Einheit ein Alarm erzeugt. Der Wert kehrt anschließend wieder in den Normalbereich zurück, es wird von der EMX-Einheit jedoch kein Alarm für das Deassertionsereignis ausgegeben. Dies kann aufgrund der Hysterese-Protokollierung von EMX auftreten. Siehe ***Was ist eine Deassertion-Hysterese?*** (siehe "***Was ist Deassertionshysterese?***" auf Seite 189)

Ereignisprotokollierung

Die EMX-Einheit erfasst standardmäßig bestimmte Systemereignisse und speichert diese in einem lokalen (internen) Ereignisprotokoll.

Anzeigen des lokalen Ereignisprotokolls

Sie können im lokalen Ereignisprotokoll bis zu 2.000 historische Ereignisse anzeigen, die auf dem EMX-Gerät aufgetreten sind.

Wenn das Protokoll bereits 2.000 Einträge enthält, überschreibt jeder neue Eintrag den jeweils ältesten Eintrag.

So zeigen Sie das lokale Protokoll an:

1. Wählen Sie "Maintenance > View Event Log" (Wartung > Ereignisprotokoll anzeigen) aus. Das Dialogfeld "Event Log" (Ereignisprotokoll) wird eingeblendet.

   Jeder Ereigniseintrag im lokalen Protokoll besteht aus:

   - Datum und Uhrzeit des Ereignisses
   - Ereignistyp
   - Beschreibung des Ereignisses
   - ID-Nummer des Ereignisses

2. Das Dialogfeld zeigt standardmäßig die letzte Seite an. Sie können:

   - Zwischen verschiedenen Seiten umschalten. Führen Sie dazu Folgendes aus:

     - Klicken Sie auf oder , um die erste oder letzte Seite anzuzeigen.

     - Klicken Sie auf oder , um die vorherige oder nächste Seite anzuzeigen.

     - Geben Sie eine Zahl in das Textfeld "Page" (Seite) ein, und drücken Sie die Eingabetaste, um eine bestimmte Seite anzuzeigen.

   - Wählen Sie einen Protokolleintrag aus der Liste aus und klicken Sie auf "Show Details" (Details anzeigen) oder doppelklicken Sie einfach auf den Protokolleintrag, um detaillierte Informationen anzuzeigen.

   Hinweis: Wenn das Dialogfeld zu klein ist, wird anstelle der Schaltfläche "Show Details" (Details anzeigen) das Symbol angezeigt. Klicken Sie in diesem Fall auf und wählen Sie "Show Details" (Details anzeigen) aus, um die Details anzuzeigen.

   - Klicken Sie auf , um das letzte Ereignis anzuzeigen.

3. Vergrößern Sie gegebenenfalls das Dialogfeld.
4. Sie können die Liste neu sortieren oder die angezeigten Spalten ändern.
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Löschen von Ereigniseinträgen

Es ist nicht notwendig, eine vorhandene Ereignishistorie aufzubewahren. Sie können sie in ihrer Gesamtheit aus dem lokalen Protokoll entfernen.

So löschen Sie alle Ereigniseinträge:

1. Wählen Sie "Maintenance > View Event Log" (Wartung > Ereignisprotokoll anzeigen) aus. Das Dialogfeld "Event Log" (Ereignisprotokoll) wird eingeblendet.
2. Klicken Sie auf "Clear Event Log" (Ereignisprotokoll löschen).
3. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Anzeigen des Kommunikationsprotokolls

Mit der EMX-Einheit können Sie die gesamte Kommunikation überprüfen, die zwischen dem EMX-Gerät und dessen grafischer Benutzeroberfläche (GUI) stattgefunden hat. Diese Informationen sind normalerweise nur für Ingenieure des technischen Supports von Interesse, und Sie brauchen diese nicht anzuzeigen.

Diese Funktion ist nur für Benutzer mit Administratorberechtigungen zugänglich.

So zeigen Sie das Kommunikationsprotokoll an:

1. Wählen Sie "Maintenance (Wartung) > View Communication Log (Kommunikationsprotokoll anzeigen)". Das Dialogfeld "Communication Log" (Kommunikationsprotokoll) wird angezeigt.
2. Das Dialogfeld zeigt standardmäßig die letzte Seite an. Sie können:
   - Zwischen verschiedenen Seiten umschalten. Führen Sie dazu Folgendes aus:

     - Klicken Sie auf oder , um die erste oder letzte Seite anzuzeigen.

     - Klicken Sie auf oder , um die vorherige oder nächste Seite anzuzeigen.

     - Geben Sie eine Zahl in das Textfeld "Page" (Seite) ein, und drücken Sie die Eingabetaste, um eine bestimmte Seite anzuzeigen.
   - Wählen Sie einen Protokolleintrag aus der Liste aus und klicken Sie auf "Show Details" (Details anzeigen) oder doppelklicken Sie einfach auf den Protokolleintrag, um detaillierte Informationen anzuzeigen.

Hinweis: Wenn das Dialogfeld zu klein ist, wird anstelle der Schaltfläche "Show Details" (Details anzeigen) das Symbol » angezeigt. Klicken Sie in diesem Fall auf » und wählen Sie "Show Details" (Details anzeigen) aus, um die Details anzuzeigen.

3. Um das Kommunikationsprotokoll sofort zu aktualisieren, klicken Sie auf .
4. Um das Kommunikationsprotokoll auf Ihrem Computer zu speichern, klicken Sie auf .
5. Vergrößern Sie gegebenenfalls das Dialogfeld.
6. Sie können die Liste neu sortieren oder die angezeigten Spalten ändern.
7. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Kapitel 8 Verwalten externer Geräte

In diesem Kapitel

Übersicht....170
Serverzugriff....170
Umgebungssensoren....173
Assetsensoren und -Tags....191
Webcams....202
GSM-Modems....208
Schroff LHX-Wärmetauscher....209

Übersicht

Die EMX-Einheit bietet Ihnen die Möglichkeit, Geräte und Bedingungen in Ihrem Rechenzentrum, z. B. den Status von Servern oder Umgebungsbedingungen, mithilfe von Sensoren und Geräten anderer Hersteller zu überwachen.

Darüber hinaus können Sie die Aktivitäten im Rechenzentrum mit einer Webcam ansehen und SMS-Nachrichten über ein GSM-Modem senden, wenn ein bestimmtes Ereignis eintritt.

Serverzugriff

Sie können überwachen, ob spezifische IT-Geräte spannungsführend sind, indem sie vom EMX-Gerät kontinuierlich angepingt werden. Die erfolgreiche Reaktion eines IT-Geräts auf den Ping-Befehl weist darauf hin, dass das IT-Gerät Spannung führt und per Fernzugriff darauf zugegriffen werden kann.

Diese Funktion ist besonders hilfreich, wenn Sie sich nicht in einem Gebiet mit Internetverbindung befinden.

Hinzufügen von IT-Geräten zur Ping-Überwachung

Sie können den Zugriff auf ein beliebiges IT-Gerät, z. B. DB-Server und Remote-Authentifizierungsserver, mit der EMX-Einheit überwachen.

So fügen Sie ein IT-Gerät für die Ping-Überwachung hinzu:

1. Wählen Sie "Device Settings" > "Server Reachability" (Geräteeinstellungen > Servererreichbarkeit). Das Dialogfeld "Server Reachability" (Servererreichbarkeit) wird angezeigt.
2. Klicken Sie auf "New" (Neu). Das Dialogfeld "Add New Server" (Neuen Server hinzufügen) wird angezeigt.

3. Standardmäßig ist das Kontrollkästchen "Enable Ping Monitoring for this Server" (Ping-Überwachung für diesen Server aktivieren) markiert. Falls nicht, markieren Sie es, um die Ping-Überwachungsfunktion zu aktivieren.
4. Geben Sie die erforderlichen Informationen an.

Feld	Beschreibung
IP Address/Hostname (IP-Adresse/Hostname)	IP-Adresse oder Hostname des IT-Geräts, dessen Zugriff Sie überwachen möchten.
Number of Successful Pings to Enable Feature (Anzahl erfolgreicher Pings zur Aktivierung der Funktion)	Anzahl erfolgreicher Pings, die notwendig sind, um diese Funktion zu aktivieren. Der gültige Bereich liegt zwischen 0 und 200.
Wait Time (in seconds) after Successful Ping (Wartezeit (in Sekunden) nach erfolgreichem Ping)	Wartezeit vor dem Senden des nächsten Ping, wenn auf den vorhergehenden Ping erfolgreich reagiert wurde. Der gültige Bereich liegt zwischen 5 und 600 (Sekunden).
Wait Time (in seconds) after Unsuccessful Ping (Wartezeit (in Sekunden) nach erfolglosem Ping)	Wartezeit vor dem Senden des nächsten Ping, wenn auf den vorhergehenden Ping nicht reagiert wurde. Der gültige Bereich liegt zwischen 3 und 600 (Sekunden).
Number of Consecutive Unsuccessful Pings for Failure (Anzahl aufeinanderfolgender erfolgloser Pings für Fehlschlag)	Anzahl aufeinanderfolgender Pings ohne Reaktion, bis das IT-Gerät als "nicht reagierend" deklariert wird. Der gültige Bereich liegt zwischen 1 und 100.
Wait Time (in seconds) before Resuming Pinging (Wartezeit (in Sekunden) vor Fortsetzen der Pings)	Wartezeit vor Fortsetzen der Pings nachdem das IT-Gerät als "nicht reagierend" deklariert wurde. Der gültige Bereich liegt zwischen 1 und 1200 (Sekunden).

5. Klicken Sie auf "OK", um die Änderungen zu speichern.
6. Zum Hinzufügen weiterer IT-Geräte wiederholen Sie Schritt 2 bis 5.
7. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Bearbeitung der Einstellungen zur Ping-Überwachung

Sie können bei Änderungsbedarf die Einstellungen zur Ping-Überwachung für jedes IT-Gerät bearbeiten.

So ändern Sie die Einstellungen zur Ping-Überwachung für ein IT-Gerät:

1. Wählen Sie "Device Settings" > "Server Reachability" (Geräteeinstellungen > Servererreichbarkeit). Das Dialogfeld "Server Reachability" (Servererreichbarkeit) wird angezeigt.
2. Klicken Sie auf das IT-Gerät, dessen Einstellungen Sie ändern möchten.
3. Klicken Sie auf "Edit" (Bearbeiten) oder doppelklicken Sie auf das IT-Gerät. Das Dialogfeld "Edit Server 'XXX'" (Server 'XXX' bearbeiten) wird angezeigt, wobei XXX die IP-Adresse oder Hostnamen des IT-Geräts darstellt.
4. Nehmen Sie an den angezeigten Informationen die Änderungen vor.
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Löschen der Einstellungen zur Ping-Überwachung

Wenn es nicht notwendig ist, den Zugriff auf ein IT-Gerät zu überwachen, entfernen Sie das Gerät.

So löschen Sie die Einstellungen zur Ping-Überwachung für ein IT-Gerät:

1. Wählen Sie "Device Settings" > "Server Reachability" (Geräteeinstellungen > Servererreichbarkeit). Das Dialogfeld "Server Reachability" (Servererreichbarkeit) wird angezeigt.
2. Klicken Sie auf das IT-Gerät, dessen Einstellungen zur Ping-Überwachung Sie entfernen möchten. Um mehrere Optionen auszuwählen, drücken Sie beim Klicken die Strg- oder Umschalttaste, um mehrere Optionen zu markieren.
3. Klicken Sie auf "Delete" (Löschen).
4. Es wird eine Meldung angezeigt, die Sie auffordert, den Vorgang zu bestätigen. Klicken Sie zum Bestätigen auf "Yes" (Ja).
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Überprüfen des Serverüberwachungsstatus

Die Ergebnisse der Serverüberwachung sind über das Dialogfeld "Server Reachability" (Servererreichbarkeit) verfügbar, wenn die Server angegeben wurden, die das EMX-Gerät überwachen soll.

So überprüfen Sie Serverüberwachungsstatus und -ergebnisse:

1. Wählen Sie "Device Settings" > "Server Reachability" (Geräteeinstellungen > Servererreichbarkeit). Das Dialogfeld "Server Reachability" (Servererreichbarkeit) wird angezeigt.
2. Die Spalte mit der Bezeichnung "Ping Enabled" (Ping aktiviert) zeigt an, ob die Überwachung für den entsprechenden Server aktiviert ist oder nicht.
   - : Dieses Symbol bedeutet, dass die Überwachung für den entsprechenden Server aktiviert ist.
   - : Dieses Symbol bedeutet, dass die Überwachung für den entsprechenden Server deaktiviert ist.
3. Die Spalte mit der Bezeichnung "Status" zeigt die Zugreifbarkeit auf jeden überwachten Server an.

Status	Beschreibung
Reachable (Erreichbar)	Auf den Server kann zugegriffen werden.
Unreachable (Unerreichbar)	Auf den Server kann nicht zugegriffen werden.
Waiting for reliable connection (Warten auf zuverlässige Verbindung)	Die Verbindung zwischen dem EMX-Gerät und dem Server ist noch nicht hergestellt.

4. Sie können die Sortierreihenfolge der Liste bei Bedarf ändern. See Ändern der Sortierreihenfolge.
5. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Umgebungssensoren

Die EMX-Einheit überwacht die Umgebungsbedingungen, wie Temperatur und Luftfeuchtigkeit, mithilfe von Umgebungssensoren.

So fügen Sie Umgebungssensoren hinzu:

1. Schließen Sie die Umgebungssensoren an das EMX-Gerät an. Siehe ***Anschließen der Umgebungssensoren (optional)*** (auf Seite 31).

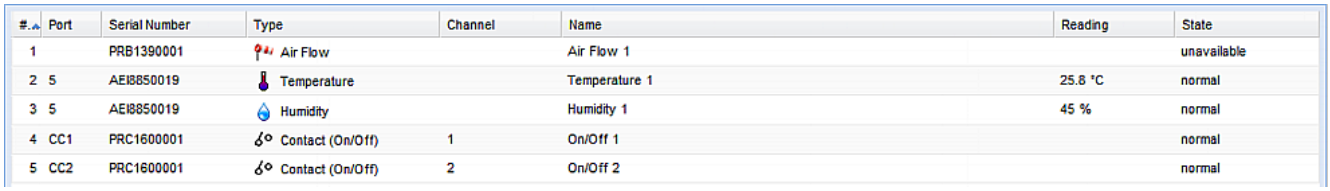
2. Melden Sie sich bei der Webschnittstelle von EMX an. Die EMX-Einheit sollte die angeschlossenen Sensoren erkannt haben und sie in der Webschnittstelle anzeigen.
3. Identifizieren Sie jeden Sensor mithilfe der jeweiligen Seriennummer. Siehe ***Festlegen von Umgebungssensoren*** (auf Seite 174).
4. Die EMX-Einheit verwaltet die erkannten Sensoren automatisch. Überprüfen Sie, ob die erkannten Sensoren verwaltet werden. Falls sie nicht verwaltet werden, lassen Sie sie verwalten. Siehe ***Verwalten von Umgebungssensoren*** (auf Seite 176).
5. Konfigurieren Sie die Sensoren. Siehe ***Konfigurieren von Umgebungssensoren*** (auf Seite 177). Folgende Schritte müssen ausgeführt werden:
   a. Benennen Sie den Sensor.
   b. Wenn es sich bei dem angeschlossenen Sensor um einen Kontaktschlusssensor von Raritan handelt, geben Sie einen geeigneten Sensortyp an.
   c. Markieren Sie den physischen Standort des Sensors im Rack oder im Raum.
   d. Konfigurieren Sie bei einem numerischen Sensor die Einstellungen für Schwellenwert, Hysterese und Zeitüberschreitung der Assertion.

Hinweis: Numerische Sensoren verwenden numerische Werte, um die Umgebungs- oder internen Bedingungen anzugeben, während Einzelsensoren (Ein/Aus-Sensoren) alphabetische Zeichen zum Beschreiben des Status verwenden. Nur numerische Sensoren verfügen über Schwellenwerteinstellungen.

Festlegen von Umgebungssensoren

Ein Umgebungssensor verfügt über ein Etikett mit der Seriennummer auf dem Sensorkabel.

Die Seriennummer jedes Sensors wird in der Webschnittstelle aufgeführt, nachdem jeder Sensor von der EMX-Einheit erkannt wurde.



#	Port	Serial Number	Type	Channel	Name	Reading	State
1		PRB1390001	Air Flow		Air Flow 1		unavailable
2	5	AEI8850019	Temperature		Temperature 1	25.8 °C	normal
3	5	AEI8850019	Humidity		Humidity 1	45 %	normal
4	CC1	PRC1600001	Contact (On/Off)	1	On/Off 1		normal
5	CC2	PRC1600001	Contact (On/Off)	2	On/Off 2		normal

Vergleichen Sie die Seriennummer auf dem Etikett mit den Seriennummern in der Sensortabelle.

Beachten Sie, dass die Informationen in den Spalten "#" und "Port" verschieden sind.

Spalte	Informationen
#	Die ID-Nummer, die jedem Umgebungssensor zugewiesen ist.
Port	Die Nummer des SENSOR-Ports, an den jeder Umgebungssensor physisch angeschlossen ist "CC1" und "CC2" beziehen sich auf den integrierten Kontaktschlusssensor-Anschluss.

Verwalten von Umgebungssensoren

Die EMX-Einheit ruft das Ergebnis eines Umgebungssensors und/oder den Status ab und zeichnet die Statusänderung auf, nachdem der Umgebungssensor verwaltet wurde.

Wenn ein Raritan-Sensorhub verwendet wird, können Sie bis zu 16 Umgebungssensoren je SENSOR-Port anschließen. Das bedeutet Folgendes:

- Für Modell EMX2-111, das nur 1 SENSOR-Port besitzt, können maximal 16 Umgebungssensoren angeschlossen werden.
- Für Modell EMX2-888, das 8 SENSOR-Ports besitzt, können maximal 128 Umgebungssensoren angeschlossen werden. Da das EMX2-888-Gerät mit zwei Channels für integrierte Kontaktschluss-Anschlüsse implementiert ist, unterstützt es maximal 130 Umgebungssensoren.
- Jeder SENSOR-Port kann nur maximal zwei Raritan-Kontaktschlusssensoren unterstützen, die das kürzeste Aktualisierungsintervall unter allen Raritan-Sensoren haben. Siehe ***Informationen zum Aktualisierungsintervall*** (auf Seite 183).

Wenn die Gesamtanzahl der verwalteten Sensoren das Maximum noch nicht erreicht hat, stellt das EMX-Gerät erkannte Umgebungssensoren automatisch unter Verwaltung. Ein Sensor muss nur manuell verwaltet werden, wenn er nicht in der Verwaltung enthalten ist.

So verwalten Sie einen Umgebungssensor manuell:

1. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie im Fenster "EMX Explorer" auf den Ordner "External Sensors" (Externe Sensoren), um die Seite "External Sensors" (Externe Sensoren) im rechten Fensterbereich zu öffnen.
3. Klicken Sie auf der Seite "External Sensors" (Externe Sensoren) auf den Sensor, den Sie verwalten möchten.

   Hinweis: Informationen zum Festlegen aller erkannten Sensoren finden Sie unter **Festlegen von Umgebungssensoren** *(auf Seite 174).*

4. Klicken Sie auf "Manage" (Verwalten). Das Dialogfeld "Manage sensor (Sensor verwalten) <serial number (Seriennummer)> (<sensor type (Sensortyp)>)" wird angezeigt, wobei <serial number> der Seriennummer des Sensors entspricht und <sensor type> den Sensortyp angibt.

Hinweis: Bei einem Kontaktschlusssensor wird hinter <sensor type> (Sensortyp) eine Channel-Nummer hinzugefügt.

5. Es gibt zwei Methoden zur Verwaltung des Sensors:
   - Um den Sensor zu verwalten, indem das EMX-Gerät ihm eine Nummer zuweist, wählen Sie "Automatically assign a sensor number" (Sensornummer automatisch zuweisen) aus. Bei dieser Methode werden keine verwalteten Sensoren freigegeben.
   - Um den Sensor zu verwalten, indem Sie ihm die gewünschte Nummer zuweisen, wählen Sie "Manually select a sensor number" (Sensornummer manuell auswählen) aus. Klicken Sie anschließend auf den Dropdown-Pfeil, um eine Nummer auszuwählen.

     Wenn die von Ihnen gewählte Nummer bereits einem Sensor zugewiesen wurde, wird dieser Sensor freigegeben, nachdem ihm die ID-Nummer entzogen wurde.

Tipp: Die Informationen in Klammern hinter jeder ID-Nummer geben an, ob die Nummer einem Sensor zugeordnet wurde. Wurde sie einem Sensor zugewiesen, zeigt sie die Seriennummer des Sensors an. Andernfalls wird "unused" (nicht verwendet) angezeigt.

6. Klicken Sie auf OK. Das EMX-Gerät beginnt, das Ergebnis und/oder den Status des Sensors zu verfolgen und anzuzeigen.
7. Zum Verwalten weiterer Sensoren wiederholen Sie die Schritte 3 bis 6.

Hinweis: Wenn die Anzahl der verwalteten Sensoren das Maximum erreicht, können Sie zusätzliche Sensoren ERST verwalten, nachdem Sie einen verwalteten Sensor entfernt oder ersetzt haben. Informationen zum Entfernen eines Sensors finden Sie unter **Entfernen von Umgebungssensoren aus der Verwaltung** *(siehe "***Aufheben der Verwaltung von Umgebungssensoren***" auf Seite 188).*

Konfigurieren von Umgebungssensoren

Sie können den Standardnamen ändern, um den verwalteten Sensor leicht zu erkennen, und seinen Ort mit X-, Y- und Z-Koordinaten beschreiben.

So konfigurieren Sie Umgebungssensoren:

1. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie im Fenster "EMX Explorer" auf den Ordner "External Sensors" (Externe Sensoren), um die Seite "External Sensors" (Externe Sensoren) im rechten Fensterbereich zu öffnen.
3. Wählen Sie den zu konfigurierenden Sensor aus.
4. Klicken Sie auf "Setup" (Einrichten). Das Dialogfeld "Setup of external sensor <serial number> (<sensor type>)" (Einrichtung des externen Sensors <Seriennummer> [<Sensortyp]>) wird angezeigt, wobei <serial number> der Seriennummer des Sensors entspricht und <sensor type> den Sensortyp angibt.

   Tipp: Sie können dieses Dialogfeld auch aufrufen, indem Sie das Symbol für den gewünschten Umgebungssensor in der Verzeichnisstruktur auswählen und dann auf der geöffneten Seite des Sensors im rechten Fensterbereich auf "Setup" (Einrichtung) klicken.

5. Wenn es sich bei dem ausgewählten Umgebungssensor um einen Raritan-Kontaktschlusssensor mit angeschlossenem Detektor/Switch eines anderen Herstellers handelt, wählen Sie im Feld "Binary Sensor Subtype" (Subtyp des Binärsensors) den entsprechenden Sensortyp aus.
   - Contact (Kontakt): Der Detektor/Switch erkennt den Türschlossstatus oder den Status "Tür offen/geschlossen".
   - Smoke Detection (Raucherkennung): Der Detektor/Switch erkennt Rauch.
   - Water Detection (Wassererkennung): Der Detektor/Switch erkennt Wasser auf dem Boden.
   - Vibration (Erschütterungen): Der Detektor/Switch erkennt Bodenerschütterungen.
6. Geben Sie im Feld "Name" einen neuen Namen ein.
7. Beschreiben Sie den Standort des Sensors, indem Sie den X-, Y- und Z-Koordinaten alphanumerische Werte zuweisen. Siehe ***Beschreiben des Sensorstandorts*** (siehe "***Beschreibung der Sensorposition***" auf Seite 180).
8. Wenn der ausgewählte Umgebungssensor ein numerischer Sensor ist, werden die Schwellenwerteinstellungen im Dialogfeld angezeigt. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf die Tabelle "Threshold Configuration" (Schwellenwertkonfiguration), um den Schwellenwert, die Deassertionshysterese und die Zeitüberschreitung der Assertion anzupassen.
   - Zum Aktivieren eines Schwellenwerts aktivieren Sie das entsprechende Kontrollkästchen. Zum Deaktivieren eines Schwellenwerts deaktivieren Sie das Kontrollkästchen.

- Nachdem Sie einen Schwellenwert aktiviert haben, geben Sie den entsprechenden numerischen Wert in das dazugehörige Textfeld ein.
- Um die Deassertionshysterese für alle Schwellenwerte zu aktivieren, geben Sie einen numerischen Wert ungleich Null in das Feld "Deassertion Hysteresis" (Deassertionshysterese) ein. Siehe ***Was ist Deassertionshysterese?*** (auf Seite 189)
- Um das Assertionszeitlimit für alle Schwellenwerte zu aktivieren, geben Sie einen numerischen Wert ungleich Null in das Feld "Assertion Timeout (samples)" (Assertionszeitlimit [Messungen]) ein. Siehe ***Was ist das Assertionszeitlimit?*** (auf Seite 190)

Wenn die in den Feldern "Upper Critical" (Oberer kritischer Schwellenwert) und "Lower Critical" (Unterer kritischer Schwellenwert) definierten Schwellenwerte erreicht werden, stuft die EMX-Einheit die Umgebungsbedingungen als kritisch und außerhalb des akzeptablen Bereichs ein.

9. Klicken Sie auf "OK", um die Änderungen zu speichern.

Einstellen des Z-Koordinatenformats

Sie können entweder die Zahl der Gestelleinheiten oder einen beschreibenden Text verwenden, um die vertikale Position (Z-Koordinaten) von Umgebungssensoren zu beschreiben.

So bestimmen Sie das Z-Koordinatenformat:

1. Klicken Sie im linken Navigationsbereich auf den Ordner "EMX". Die Seite "Settings" (Einstellungen) wird angezeigt.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie auf der Seite "Settings" (Einstellungen) auf "Setup" (Einrichten). Das Dialogfeld "EMX Setup" (EMX einrichten) wird eingeblendet.
3. Klicken Sie im Feld "External sensors Z coordinate format" (Externe Sensoren – Z-Koordinatenformat) auf den Dropdown-Pfeil, und wählen Sie eine Option aus der Liste.
   - Rack Units (Gestelleinheiten): Die Höhe der Z-Koordinate wird in Standard-Rackeinheiten gemessen. Wenn diese Option ausgewählt ist, können Sie einen numerischen Wert für die Rackeinheit eingeben, um die Z-Koordinate von beliebigen Umgebungssensoren zu beschreiben.
   - Free-Form (Freie Form): Zum Angeben der Z-Koordinate können Sie einen beliebigen alphanumerischen String verwenden.
4. Klicken Sie auf "OK", um die Änderungen zu speichern.

Beschreibung der Sensorposition

Verwenden Sie die X-, Y- und Z-Koordinaten, um den physischen Standort jedes Sensors zu beschreiben. Mithilfe dieser Standortwerte können Sie die Datensätze der Umgebungsbedingungen an festen Standorten für Ihre IT-Geräte verfolgen. Die X-, Y- und Z-Werte dienen als zusätzliche Attribute und sind nicht an ein bestimmtes Maßeinheitensystem gebunden. Sie können auch andere Werte als Maßeinheiten verwenden. Beispiel:

X = *Zeile für braunes Gestell*

Y = *Drittes Rack*

Z = *Oberseite des Gestells*

Die Werte für die X-, Y- und Z-Koordinaten können Folgendes enthalten:

- Für X und Y: Eine Kombination aus alphanumerischen Zeichen. Der Koordinatenwert kann 0 bis 24 Zeichen umfassen.
- Wenn das Format für die Z-Koordinate auf *Rack Units* (Gestelleinheiten) eingestellt ist, kann Z einen beliebigen Wert von 0 bis 60 annehmen.
- Wenn das Format für die Z-Koordinate auf *Free-Form* (Freie Form) eingestellt ist, sind für Z 0 bis 24 alphanumerische Zeichen möglich.

Tipp: Informationen zum Konfigurieren und Abrufen dieser Koordinatenwerte über SNMP finden Sie in der EMX-MIB. Informationen zum Konfigurieren und Abrufen dieser Werte über die Befehlszeilenschnittstelle (CLI) finden Sie unter Verwenden der Befehlszeilenschnittstelle.

Einrichten der Datenprotokollierung

Das EMX-Gerät kann 120 Messungen für jeden Sensor in einem Speicherpuffer speichern. Dieser Speicherpuffer wird als Datenprotokoll bezeichnet. Die Sensormesswerte im Datenprotokoll können über SNMP abgerufen werden.

Über das Feld "Measurements Per Log Entry" (Ergebnisse pro Protokolleintrag) können Sie konfigurieren, wie oft Messungen in das Datenprotokoll eingetragen werden. Da die Umgebungssensoren jede Sekunde gemessen werden, würde die Angabe des Wertes 60 zum Beispiel bedeuten, dass die Messwerte einmal pro Minute in das Datenprotokoll eingetragen werden. Da es 120 Messungen pro Sensor gibt, bedeutet die Angabe "60", dass das Protokoll die letzten zwei Stunden der Messungen speichern kann, bevor die ältesten Einträge im Protokoll überschrieben werden.

Obwohl die Umgebungssensoren jede Sekunde gemessen werden, werden ihre Ergebnisse möglicherweise nicht jede Sekunde aktualisiert. Siehe ***Informationen zum Aktualisierungsintervall*** (auf Seite 183). Das Aktualisierungsintervall variiert abhängig von der Anzahl der Umgebungssensoren, die an das EMX-Gerät angeschlossen sind, sowie vom Sensortyp. Je mehr Umgebungssensoren angeschlossen ist, desto größer ist das Aktualisierungsintervall. Geben Sie daher einen hohen Wert in das Feld "Measurements Per Log Entry" (Messungen pro Protokolleintrag) ein, wenn viele Umgebungssensoren angeschlossen sind.

Bei jeder Eintragung von Messwerten in das Protokoll werden drei Werte für jeden Sensor eingetragen: der Durchschnittswert, das Minimum und das Maximum. Wenn die Messwerte z. B. jede Minute eingetragen werden, wird der Durchschnitt der Messwerte der vorhergehenden 60 Sekunden zusammen mit dem Minimum und dem Maximum der Messwerte in das Protokoll eingetragen.

Hinweis: Damit dieses Feature genutzt werden kann, muss der SNMP-Agent der EMX-Einheit aktiviert sein. Weitere Informationen finden Sie unter **Aktivieren von SNMP** *(auf Seite 217). Durch die Verwendung eines NTP-Zeitservers stellen Sie außerdem sicher, dass die Messungen über einen korrekten Zeitstempel verfügen.*

Aktivieren der Datenprotokollierung

Standardmäßig ist die Option "Data Logging" (Datenprotokollierung) deaktiviert. Nur Benutzer mit der Berechtigung "Administrator" oder "Change Data Logging Settings" (Einstellungen für Datenprotokollierung ändern) können dieses Feature aktivieren oder deaktivieren. Siehe ***Einrichten von Benutzerfunktionen*** (auf Seite 70).

So konfigurieren Sie die Datenprotokollierung:

1. Wählen Sie "Device Settings" > "Data Logging" (Geräteeinstellungen > Datenprotokollierung) aus. Das Dialogfeld "Data Logging Options" (Optionen für die Datenprotokollierung) wird eingeblendet.
2. Um die Datenprotokollierung zu aktivieren, wählen Sie im Feld "Enable Data Logging" (Datenprotokollierung aktivieren) das Kontrollkästchen "enable" (aktivieren) aus.
3. Geben Sie im Feld "Measurements Per Log Entry" (Ergebnisse pro Protokolleintrag) einen Wert ein. Der gültige Bereich liegt zwischen 1 und 600. Der Standardwert ist 60.
4. Wählen Sie die Umgebungssensoren aus, deren Datenprotokollierung Sie aktivieren möchten.
   - Zur Auswahl eines Teils der Sensoren aktivieren Sie die Kontrollkästchen der gewünschten Sensoren in der Spalte "Logging Enabled" (Protokollierung aktiviert).
   - Um alle Sensoren auszuwählen, klicken Sie auf "Enable All" (Alles aktivieren) oder "Enable All in Page" (Alle auf der Seite aktivieren).
   - Um die Auswahl aller Sensoren rückgängig zu machen, klicken Sie auf "Disable All" (Alles deaktivieren) oder "Disable All in Page" (Alle auf der Seite deaktivieren).
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Informationen zum Aktualisierungsintervall

Umgebungssensoren von Raritan lassen sich entsprechend dem Aktualisierungsintervall des Sensorergebnisses oder -status in zwei Kategorien unterteilen.

- Normaler Typ: Sensorergebnisse oder -zustände werden in einem längeren Intervall aktualisiert, das entsprechend der Gesamtanzahl der angeschlossenen Umgebungssensoren zwischen 3 bis 40 Sekunden variiert. Die meisten Umgebungssensoren von Raritan gehören zu diesem Typ, z. B. Temperatur- oder Feuchtigkeitssensoren.
- Typ hoher Priorität: Sensorergebnisse oder -zustände werden in einem kürzeren Intervall aktualisiert, das kleiner oder gleich 3 Sekunden ist. Kontaktschlusssensoren von Raritan gehören zu diesem Typ.

Anzeigen von Sensordaten

Die Messwerte von Umgebungssensoren werden auf der Webschnittselle angezeigt, nachdem die Sensoren korrekt angeschlossen und verwaltet wurden.

Die Seite "Dashboard" zeigt nur Informationen zu verwalteten Umgebungssensoren an, während die Seite "External Sensors" (Externe Sensoren) Informationen zu verwalteten und nicht verwalteten Sensoren anzeigt.

Eine farbig dargestellte Zeile mit einem Sensorergebnis weist darauf hin, dass das Sensorergebnis bereits einen Schwellenwert über- oder unterschreitet oder dass mindestens ein integrierter LHX-Sensor am Wärmetauscher ausgefallen ist. Siehe ***Gelb oder Rot hervorgehobene Ergebnisse (EMX)*** (siehe "***Gelb oder Rot hervorgehobene Ergebnisse***" auf Seite 58).

So zeigen Sie nur verwaltete Umgebungssensoren an:

1. Klicken Sie im Fenster "EMX Explorer" auf das Dashboard-Symbol, um die Seite "Dashboard" im rechten Fensterbereich zu öffnen.
2. Suchen Sie den Abschnitt "External Sensors" (Externe Sensoren) auf der Seite "Dashboard". Dieser Abschnitt zeigt:
   - Die Gesamtanzahl der verwalteten Sensoren
   - Die Gesamtanzahl der nicht verwalteten Sensoren
   - Informationen zu jedem verwalteten Sensor, einschließlich:
     - Name
     - Messwert
     - Status

So zeigen Sie sowohl verwaltete als auch nicht verwaltete Umgebungssensoren an:

1. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie im Fenster "EMX Explorer" auf den Ordner "External Sensors" (Externe Sensoren), um die Seite "External Sensors" (Externe Sensoren) im rechten Fensterbereich zu öffnen.

   Es werden detaillierte Informationen zu jedem angeschlossenen Sensor angezeigt, einschließlich:

   - Bezeichnung (Nummer)
   - Seriennummer
   - Sensortyp
   - Name
   - Messwert
   - Status
   - Channel (nur bei Kontaktschlusssensoren)

Sensormessgenauigkeit

Raritan-Umgebungssensoren verfügen über die folgenden werkseitigen Spezifikationen. Eine Kalibrierung der Umgebungssensoren ist nicht erforderlich.

- Temperatur: +/-2%
- Feuchtigkeit: +/-5%
- Differenzluftdruck: +/-1.5%
- Luftstrom: +/-6.5%

Status verwalteter Sensoren

Ein Umgebungssensor zeigt den Status an, wenn er verwaltet wird.

Die verfügbaren Sensorzustände variieren abhängig vom Sensortyp (numerischer Sensor oder Einzelsensor). Ein Kontaktschlusssensor ist ein Einzelsensor. Folglich wechselt er nur zwischen drei Zuständen, "unavailable" (nicht verfügbar), "alarmed" (Alarmzustand) und "normal".

Hinweis: Numerische Sensoren verwenden numerische Werte, um die Umgebungs- oder internen Bedingungen anzugeben, während Einzelsensoren (Ein/Aus-Sensoren) alphabetische Zeichen zum Beschreiben des Status verwenden.

Sensorstatus	Anwendungsbereich
unavailable (nicht verfügbar)	Alle Sensoren
alarmed (Alarmzustand)	Einzelsensoren
normal	Alle Sensoren
below lower critical (unter unterem kritischen Schwellenwert)	Numerische Sensoren
below lower warning (unter unterem Warnschwellenwert)	Numerische Sensoren
above upper warning (über oberem Warnschwellenwert)	Numerische Sensoren
above upper critical (über oberem kritischen Schwellenwert)	Numerische Sensoren

Status "unavailable" (nicht verfügbar)

Der Status *unavailable* (nicht verfügbar) gibt an, dass die Verbindung zum Sensor unterbrochen wurde.

Die EMX-Einheit überprüft alle verwalteten Sensoren in regelmäßigen Abständen (Sekunden) mit Ping. Wird ein bestimmter Sensor bei drei aufeinanderfolgenden Überprüfungen nicht erkannt, wird der Status *unavailable* (nicht verfügbar) für diesen Sensor angezeigt.

Wird die Kommunikation mit dem Prozessor eines Kontaktschlusssensors unterbrochen, haben alle Detektoren (d. h. alle Switches), die an dasselbe Sensormodul angeschlossen sind, den Status "unavailable" (nicht verfügbar).

Hinweis: Wenn der Sensor als nicht verfügbar betrachtet wird, bleibt die bestehende Sensorkonfiguration unverändert. So bleibt z. B. die ID-Nummer, die dem Sensor zugeordnet wurde, dem Sensor weiterhin zugeordnet.

Die EMX-Einheit überprüft nicht verfügbare Sensoren weiterhin mit Ping und beendet den Status *unavailable* (nicht verfügbar), nachdem der Sensor bei zwei aufeinanderfolgenden Überprüfungen erkannt wurde.

Status "normal"

Dieser Status gibt an, dass sich der Sensor im Normalzustand befindet.

Bei einem Kontaktschlusssensor ist dieser Status der Normalzustand, den Sie festgelegt haben.

- Wenn der Normalzustand auf "Normally Closed" (Normalerweise geschlossen) festgelegt ist, bedeutet der Status *normal*, dass der Kontaktschlussschalter geschlossen ist.
- Wenn der Normalzustand auf "Normally Open" (Normalerweise offen) festgelegt ist, bedeutet der Status *normal*, dass der Kontaktschlussschalter offen ist.

Hinweis: Informationen zum Festlegen des Normalzustands finden Sie unter **Konfigurieren eines Kontaktschlusssensors** *(auf Seite 35). Informationen zum Festlegen des Normalzustands beim Anschluss integrierter Kontaktschlusssensoren finden Sie unter* **Anschluss von Detektoren/Switches anderer Hersteller an das EMX-Gerät** *(auf Seite 36).*

Bei einem numerischen Sensor bedeutet dieser Status, dass das Sensormessergebnis wie unten angegeben innerhalb des akzeptablen Bereichs liegt:

Unterer Warnschwellenwert <= Messergebnis < Oberer Warnschwellenwert

---

Hinweis: Das Symbol <= bedeutet kleiner (<) oder gleich (=).

Status "alarmed" (Alarmzustand)

Dieser Status gibt an, dass sich ein Einzelsensor (Ein/Aus-Sensor) im "abnormen" Zustand befindet.

Bei einem Kontaktschlusssensor richtet sich die Bedeutung dieses Status nach der Einstellung für den Normalzustand des Sensors.

- Wenn der Normalzustand auf "Normally Closed" (Normalerweise geschlossen) festgelegt ist, bedeutet der Status *alarmed* (Alarmzustand), dass der Kontaktschlussschalter offen ist.
- Wenn der Normalzustand auf "Normally Open" (Normalerweise offen) festgelegt ist, bedeutet der Status *alarmed* (Alarmzustand), dass der Kontaktschlussschalter geschlossen ist.

Hinweis: Informationen zum Festlegen des Normalzustands finden Sie unter **Konfigurieren eines Kontaktschlusssensors** *(auf Seite 35). Informationen zum Festlegen des Normalzustands beim Anschluss integrierter Kontaktschlusssensoren finden Sie unter* **Anschluss von Detektoren/Switches anderer Hersteller an das EMX-Gerät** *(auf Seite 36).*

Tipp: Die LED eines Kontaktschlusssensors leuchtet im Status alarmed *(Alarmzustand). Wenn das Sensormodul zwei Kanäle für den Anschluss zweier Schalter besitzt, sind zwei LEDs verfügbar. Prüfen Sie anhand der Channel-Nummer der LED, welcher Kontaktschlussschalter sich im "abnormen" Zustand befindet.*

Status "below lower critical"

Dieser Status gibt an, dass das Messergebnis eines numerischen Sensors wie unten gezeigt unter dem unteren kritischen Schwellenwert liegt:

Ergebnis < Unterer kritischer Schwellenwert

Status "below lower warning"

Dieser Status gibt an, dass das Messergebnis eines numerischen Sensors wie unten gezeigt unter dem unteren Warnschwellenwert liegt:

Unterer kritischer Schwellenwert <= Messergebnis < Unterer Warnschwellenwert

---

Hinweis: Das Symbol <= bedeutet kleiner (<) oder gleich (=).

Status "above upper warning"

Dieser Status gibt an, dass das Messergebnis eines numerischen Sensors wie unten gezeigt über dem oberen Warnschwellenwert liegt:

Oberer Warnschwellenwert <= Messergebnis < Oberer kritischer Schwellenwert

Hinweis: Das Symbol <= bedeutet kleiner (<) oder gleich (=).

Status "above upper critical"

Dieser Status gibt an, dass das Messergebnis eines numerischen Sensors wie unten gezeigt über dem oberen kritischen Schwellenwert liegt:

Oberer kritischer Schwellenwert <= Ergebnis

Hinweis: Das Symbol <= bedeutet kleiner (<) oder gleich (=).

Aufheben der Verwaltung von Umgebungssensoren

Wenn ein bestimmter Umgebungsfaktor nicht überwacht werden muss, können Sie den entsprechenden Umgebungssensor aus der Verwaltung entfernen oder freigeben, so dass das EMX-Gerät keine weiteren Messungen und/oder Status des Sensors abruft.

So geben Sie einen verwalteten Sensor frei:

1. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie im Fenster "EMX Explorer" auf den Ordner "External Sensors" (Externe Sensoren), um die Seite "External Sensors" (Externe Sensoren) im rechten Fensterbereich zu öffnen.
3. Klicken Sie auf der Seite "External Sensors" (Externe Sensoren) auf den Sensor, der nicht mehr verwaltet werden soll.
4. Klicken Sie auf "Release" (Freigeben).

Nachdem ein Sensor aus der Verwaltung entfernt wurde, wird die dem Sensor zugewiesene ID-Nummer freigegeben und kann automatisch einem neu erkannten Sensor zugewiesen werden.

Schwellenwertinformationen

Nach dem Festlegen und Aktivieren der Schwellenwerte generiert das EMX-Gerät Alarmbenachrichtigungen, sobald der Status eines Sensors einen Schwellenwert erreicht.

Für jeden Sensor gibt es vier Schwellenwerte: Unterer kritischer Schwellenwert, unterer und oberer Warnschwellenwert sowie oberer kritischer Schwellenwert.

- Die oberen und unteren Warnschwellenwerte zeigen an, dass das Sensorergebnis den Warnbereich vor dem kritischen Schwellenwert erreicht hat.
- Die oberen und unteren kritischen Schwellenwerte zeigen an, dass das Sensorergebnis eine kritische Stufe erreicht hat.

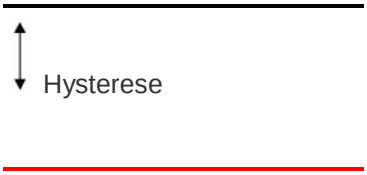
Um das Erzeugen vieler Alarmereignisse zu vermeiden, wird die Deassertionshysterese für jeden Schwellenwert aktiviert. Sie können gegebenenfalls den Standardwert der Hysterese ändern. Weitere Informationen zur Deassertionshysterese finden Sie unter ***Was ist Deassertionshysterese?*** (auf Seite 189).

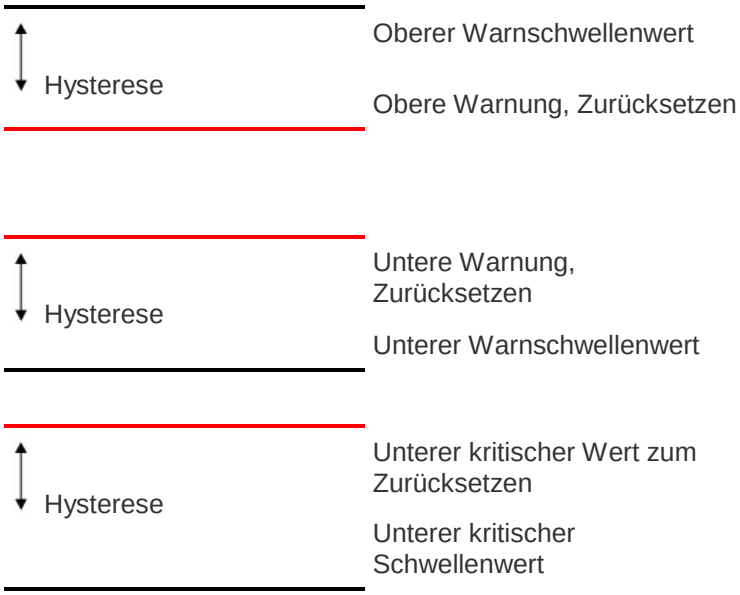
Hinweis: Nachdem Sie die Schwellenwerte festgelegt haben, müssen die Ereignisregeln konfiguriert werden. Siehe **Konfigurieren von Ereignisregeln** *(siehe "***Ereignisregeln und Aktionen***" auf Seite 137).*

Informationen zum Konfigurieren des Schwellenwerts für einen Umgebungssensor finden Sie unter ***Konfigurieren von Umgebungssensoren*** (auf Seite 177). Informationen zum Konfigurieren von Schwellenwerten für einen Schroff LHX-Wärmetauscher finden Sie unter ***Konfigurieren von Temperatur- und Lüfterschwellenwerten*** (auf Seite 211).

Was ist Deassertionshysterese?

Durch die Hysterese-Einstellung wird festgelegt, wann ein Schwellenwertvorfall zurückgesetzt wird. Im folgenden Diagramm wird dargestellt, wie Hysterese-Werte mit Schwellenwerten zusammenhängen:





Die Hysterese-Werte definieren einen Schwellenwert zum Zurücksetzen. Bei den oberen Schwellenwerten muss das Messergebnis unter diesen Schwellenwert zum Zurücksetzen fallen, bevor ein Deassertionsereignis erzeugt wird. Bei den unteren Schwellenwerten muss das Messergebnis über diesen Schwellenwert zum Zurücksetzen steigen, bevor ein Deassertionsereignis erzeugt wird.

Was ist das Assertionszeitlimit?

Wenn das Assertionszeitlimit aktiviert ist, führt das EMX-Gerät bei einer Warn- oder kritischen Bedingung lediglich nach einer angegebenen Anzahl aufeinanderfolgender Messungen, die einen bestimmten Schwellenwert über- oder unterschreiten, eine Assertion durch. Damit wird verhindert, dass eine Reihe von Schwellenwertalarmen generiert wird, wenn die Messergebnisse gleich nach Überschreiten eines oberen Schwellenwerts oder Unterschreiten einen unteren Schwellenwerts wieder normal sind.

Assetsensoren und -Tags

Ein Feature-Port ist mit einer Kombination aus dem Namen "Asset Strip" und der Port-Nummer gekennzeichnet.

Nachdem Sie einen Assetsensor angeschlossen haben, müssen Sie die Gesamtanzahl der Rackeinheiten (Tag-Ports) zwischen dem angeschlossenen Assetsensor und dem EMX-Gerät angeben.

Bei Bedarf können Sie die Einstellungen für die LED-Farbe für eine bestimmte Rackeinheit am Assetsensor auch manuell ändern, damit sich die LED anders verhält als andere LEDs.

Die EMX-Einheit unterstützt die Verkettung von AMS-M2-Z-Assetsensoren. Informationen zu Einschränkungen bei der Verkettung von AMS-M2-Z-Assetsensoren finden Sie unter ***Einschränkungen beim Verketten von AMS-M2-Z-Sensoren*** (auf Seite 197). Nach dem Anschließen erkennt die EMX-Einheit die einzelnen AMS-M2-Z-Assetsensoren, die Teil der Reihe sind. Bei Bedarf können Blade-Erweiterungen an jeden AMS-M2-Z-Assetsensor in der Reihe angeschlossen werden. Beim Hinzufügen oder Entfernen von AMS-M2-Z-Assetsensoren zu bzw. aus der Reihe werden in EMX Ereignisse generiert.

Konfigurieren des Assetsensors

Die EMX-Einheit KANN NICHT erkennen, wie viele Rackeinheiten (Tag-Ports) ein verbundener Assetsensor unterstützt. Sie müssen diese Information manuell eingeben.

Außerdem können Sie dem Assetsensor einen Namen zuweisen oder die Nummerierung für alle Rackeinheiten in der Webschnittstelle festlegen. Zudem können Sie eine Beschreibung angeben, um die einzelnen Assetsensoren zu identifizieren.

Nach dem benutzerdefinierten Namen folgt die Bezeichnung in Klammern.

Hinweis: In diesem Kontext bezieht sich die Kennung auf die Port-Nummer, an der der Assetsensor angeschlossen ist.

So konfigurieren Sie einen Assetsensor:

1. Falls noch nicht geschehen, schließen Sie den Assetsensor an die EMX-Einheit an. Siehe ***Anschließen von Assetsensoren an das EMX-Gerät*** (auf Seite 24).
2. Klicken Sie in der Navigationsstruktur auf den Ordner "Feature Ports" (Feature-Ports), um ihn zu erweitern.

3. Klicken Sie auf den gewünschten Assetsensor. Die für diesen Assetsensor spezifische Seite wird im rechten Fensterbereich geöffnet. Sie enthält die Einstellungen des Assetsensors sowie Informationen aller Rackeinheiten (Tag-Ports).

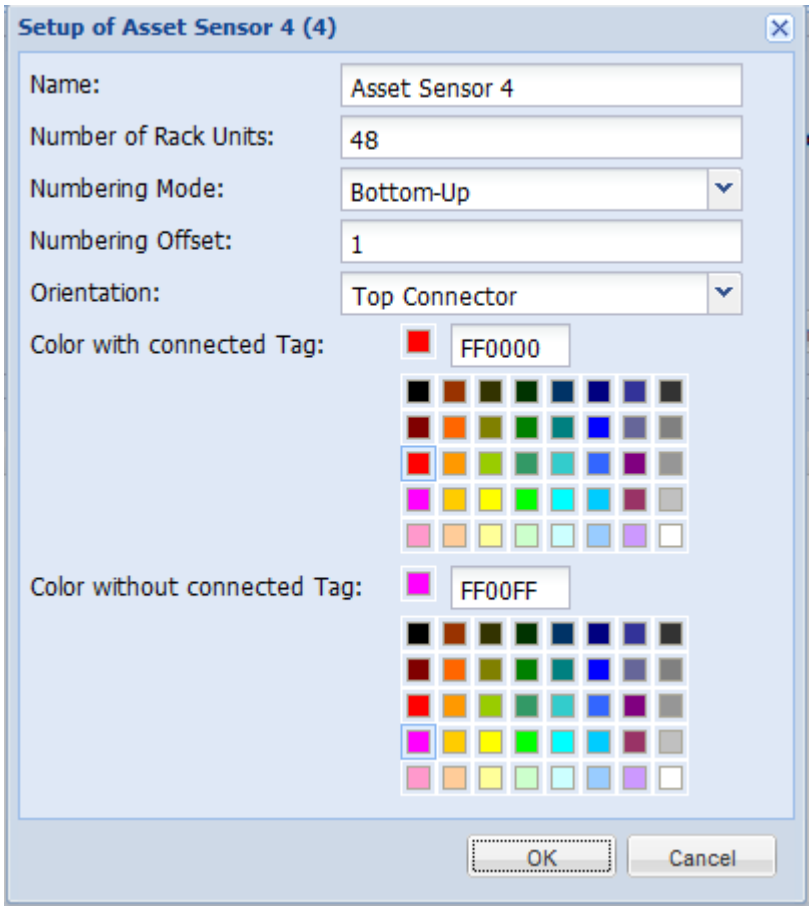
   Hinweis: Sie können das Dialogfeld auch aufrufen, indem Sie auf den Assetsensor doppelklicken, der auf der Seite "Dashboard" angezeigt wird.

4. Klicken Sie im Bereich "Settings" (Einstellungen) auf "Setup" (Einrichtung). Das Dialogfeld "Setup of Asset Strip" (Assetstrip einrichten) wird angezeigt.
5. Geben Sie einen Namen für den Assetsensor ein.
6. Geben Sie die Gesamtanzahl der Rackeinheiten, über die der ausgewählte Assetsensor verfügt, in das Feld "Number of Rack Units" (Anzahl der Rackeinheiten) ein. In diesem Feld wird standardmäßig der Wert 48 angezeigt.
7. Legen Sie fest, wie alle Rackeinheiten auf dem Assetsensor nummeriert werden sollen. Wählen Sie dazu bei "Numbering Mode" (Nummerierungsmodus) eine Option aus.
   - Top-Down (Von oben nach unten): Die Rackeinheiten sind in aufsteigender Reihenfolge von oben nach unten nummeriert.
   - Bottom-Up (Von unten nach oben): Die Rackeinheiten sind in absteigender Reihenfolge von oben nach unten nummeriert.
8. Wählen Sie im Feld "Numbering Offset" (Nummerierungsverschiebung) die Anfangsnummer aus. Wenn Sie z. B. 3 auswählen, hat die erste Rackeinheit die Nummer 3, die zweite die Nummer 4, die dritte die Nummer 5 usw. bis zur letzten Nummer.
9. Geben Sie im Feld "Orientation" (Ausrichtung) an, wie der Assetsensor in das Rack eingebaut ist. Die Rackeinheit, die dem RJ-45-Anschluss des Assetsensors am nächsten ist, wird in der Webschnittstelle mit der Indexnummer 1 gekennzeichnet.

   Bei der neuesten Version von Assetsensoren mit integriertem Neigungssensor muss die Ausrichtung NICHT manuell konfiguriert werden. Das EMX-Gerät erkennt die Ausrichtung der Assetsensoren und konfiguriert sie automatisch.

   - Top Connector (Anschluss oben): Diese Option gibt an, dass der Assetsensor so montiert ist, dass sich der RJ-45-Anschluss oben befindet.
   - Bottom Connector (Anschluss unten): Diese Option gibt an, dass der Assetsensor so montiert ist, dass sich der RJ-45-Anschluss unten befindet.

10. Um die LED-Farbe zu ändern, die das Vorhandensein eines angeschlossenen Tags angibt, klicken Sie entweder auf eine Farbe in der Farbpalette oder geben Sie den hexadezimalen RGB-Wert der Farbe in das Feld "Color with connected Tag" (Farbe bei angeschlossenem Tag) ein.
11. Um die LED-Farbe zu ändern, die das Nichtvorhandensein eines angeschlossenen Tags angibt, klicken Sie entweder auf eine Farbe in der Farbpalette oder geben Sie den hexadezimalen RGB-Wert der Farbe in das Feld "Color without connected Tag" (Farbe ohne angeschlossenes Tag) ein.
12. Klicken Sie auf "OK", um die Änderungen zu speichern.



Ändern der Farbeinstellungen einer bestimmten LED

In der EMX-Webschnittstelle bezieht sich eine Rackeinheit auf einen Tag-Port am Assetsensor. Sie können eine bestimmte Rackeinheit angeben oder die Einstellungen für die LED-Farbe ändern, sodass sich diese LED anders verhält als andere am selben Assetsensor.

So ändern Sie die Einstellungen einer LED:

1. Falls noch nicht geschehen, schließen Sie den Assetsensor an die EMX-Einheit an. Siehe ***Anschließen von Assetsensoren an das EMX-Gerät*** (auf Seite 24).
2. Klicken Sie in der Navigationsstruktur auf den Ordner "Feature Ports" (Feature-Ports), um ihn zu erweitern.
3. Klicken Sie auf den gewünschten Assetsensor. Die für diesen Assetsensor spezifische Seite wird im rechten Fensterbereich geöffnet. Sie enthält die Einstellungen des Assetsensors sowie Informationen aller Rackeinheiten (Tag-Ports).

   Hinweis: Sie können das Dialogfeld auch aufrufen, indem Sie auf den Assetsensor doppelklicken, der auf der Seite "Dashboard" angezeigt wird.
4. Wählen Sie die Rackeinheit aus, deren LED-Einstellungen Sie ändern möchten.
5. Klicken Sie auf "Configure Rack Unit" (Rackeinheit konfigurieren) oder doppelklicken Sie auf die ausgewählte Rackeinheit. Für die ausgewählte Rackeinheit wird ein Dialogfeld für das Einrichten angezeigt.
6. Geben Sie im Feld "Name" einen Namen ein, um diese Rackeinheit zu kennzeichnen.
7. Wählen Sie für den LED-Modus dieser Rackeinheit entweder "Auto" (Automatisch) oder "Manual Override" (Manuelles Überschreiben).
   - Auto (automatisch) (auf Grundlage des Tag): Dies ist die Standardeinstellung. Wenn diese Option ausgewählt ist, entspricht die LED den globalen LED-Farbeinstellungen.
   - Manual Override (Manuelles Überschreiben): Mit dieser Option wird das Verhalten dieser LED geändert. Nach Auswahl dieser Option müssen Sie einen LED-Modus und/oder eine LED-Farbe für die ausgewählte Rackeinheit auswählen.

- LED Mode (LED-Modus): Wählen Sie "On" (Ein), wenn die LED leuchten soll, "Off" (Aus), wenn die LED nicht leuchten soll, "Slow blinking" (Langsam blinkend), wenn die LED langsam blinken soll, oder "Fast blinking" (Schnell blinkend), wenn sie schnell blinken soll.
- LED Color (LED-Farbe): Wenn Sie im Feld "LED Mode" (LED-Modus) "On" (Ein), "Slow blinking" (Langsam blinkend) oder "Fast blinking" (Schnell blinkend) wählen, legen Sie eine LED-Farbe fest, indem Sie entweder auf eine Farbe in der Farbpalette klicken oder den hexadezimalen RGB-Wert einer Farbe in das dazugehörige Textfeld eingeben.

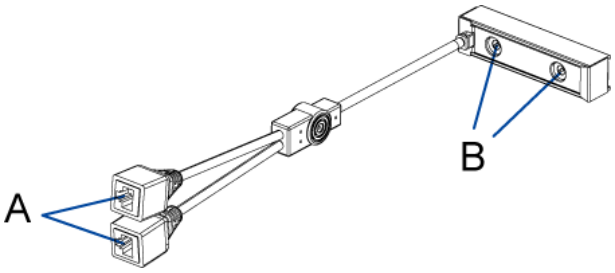
8. Klicken Sie auf "OK", um die Änderungen zu speichern.

Anschließen von AMS-M2-Z-Assetsensoren (optional)

Der AMS-M2-Z ist ein besonderer Typ eines Assetsensors, der – mit dem folgenden Unterschied – wie normale MASTER-Assetsensoren funktioniert.

- Er stellt zwei RJ-45-Anschlüsse bereit.
- Es besteht die Möglichkeit, mehrere AMS-M2-Z-Assetsensoren zu verketten.
- An jedem AMS-M2-Z sind nur zwei Tag-Ports verfügbar, sodass nur zwei Asset-Tags angeschlossen werden können.

Dieses Produkt eignet sich besonders zum Überwachen großer Geräte wie SAN-Boxes im Schrank.



Position	Beschreibung
A	RJ-45-Anschlüsse
B	Tag-Ports

So schließen Sie AMS-M2-Z-Assetsensoren an die EMX-Einheit an:

1. Schließen Sie den AMS-M2-Z über ein Kabel der Kategorie 5e/6 an die EMX-Einheit an.
   a. Schließen Sie ein Ende des Kabels an den RJ-45-Port mit der Beschriftung "Input" (Eingang) am AMS-M2-Z an.

b. Schließen Sie das andere Ende des Kabels an den FEATURE-Port der EMX-Einheit an.

2. Befestigen Sie das Asset-Tag am IT-Gerät, und schließen Sie das Asset-Tag am AMS-M2-Z an, indem Sie den Tag-Stecker mit dem Tag-Port am AMS-M2-Z verbinden. Weitere Informationen finden Sie unter ***Anschließen von Asset-Sensoren an das EMX-Gerät*** (siehe "***Anschließen von Assetsensoren an das EMX-Gerät***" auf Seite 24).

3. Falls erforderlich, verketten Sie mehrere AMS-M2-Z, um mehr als zwei IT-Geräte über diese EMX-Einheit zu verfolgen.

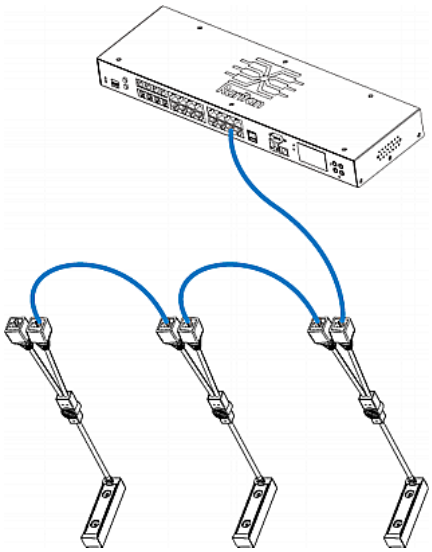
   a. Prüfen Sie, ob die Länge des Kabels der Kategorie 5e/6 innerhalb der Grenzen liegt. Informationen zu Einschränkungen bei der Kabellänge finden Sie unter ***Einschränkungen beim Verketten von AMS-M2-Z-Sensoren*** (auf Seite 197).

   b. Verbinden Sie ein Ende des Kabels der Kategorie 5e/6 mit dem RJ-45-Anschluss mit der Beschriftung "Output" (Ausgang) des AMS-M2-Z, der an die EMX-Einheit angeschlossen wird.

   c. Schließen Sie das andere Ende des Kabels an den RJ-45-Anschluss mit der Beschriftung "Input" (Eingang) an einem anderen AMS-M2-Z an.

   d. Wiederholen Sie die oben beschriebenen Schritte, um weitere AMS-M2-Z-Sensoren zu verketten. Informationen zur maximalen Anzahl an AMS-M2-Z-Assetsensoren, die verkettet werden können, finden Sie unter ***Einschränkungen beim Verketten von AMS-M2-Z-Sensoren*** (auf Seite 197).

   e. Um das Gewicht aller Verbindungskabel halten zu können, empfiehlt es sich dringend, die Kabelbinder zu verwenden.



4. Wiederholen Sie Schritt 2, um IT-Geräte über die Asset-Tags an die anderen AMS-M2-Z-Sensoren in der Reihe anzuschließen.

Einschränkungen beim Verketten von AMS-M2-Z-Sensoren

Beim Verketten von AMS-M2-Z-Assetsensoren gibt es ein paar Einschränkungen. Diese variieren abhängig vom Raritan-Produktmodell, das an den ersten AMS-M2-Z-Sensor angeschlossen ist.

Modelle	Einschränkungen beim Verketten
Alle PDUs, deren Modellname mit PX2 beginnt	• Es können bis zu vier AMS-M2-Z verkettet werden. • Die maximale Kabellänge zwischen jedem AMS-M2-Z in der Reihe beträgt zwei Meter.
EMX2-111	• Es können bis zu zwei AMS-M2-Z verkettet werden. • Die maximale Kabellänge zwischen jedem AMS-M2-Z in der Reihe beträgt zwei Meter.
EMX2-888	• Es können bis zu sechs AMS-M2-Z verkettet werden. • Die maximale Kabellänge zwischen jedem AMS-M2-Z in der Reihe beträgt drei Meter.

Erweitern eines Blade-Erweiterungsstrips

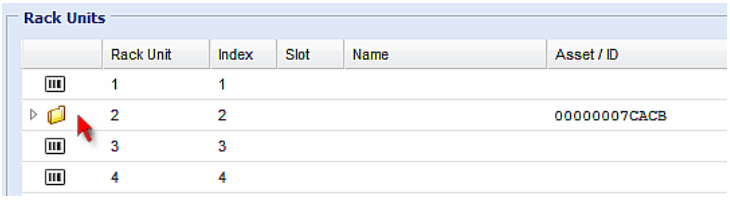
Genauso wie ein Assetsensor verfügt auch ein Blade-Erweiterungsstrip über mehrere Tag-Ports. Nachdem Sie ihn an einen bestimmten Assetsensor angeschlossen haben, wird er als Ordner auf der Seite des Assetsensors angezeigt.

Hinweis: Wenn Sie den Tag-Stecker des Blade-Erweiterungsstrips vorübergehend abziehen müssen, warten Sie mindestens 1 Sekunde, bevor Sie ihn wieder anschließen, weil die EMX-Einheit ihn sonst nicht erkennt.

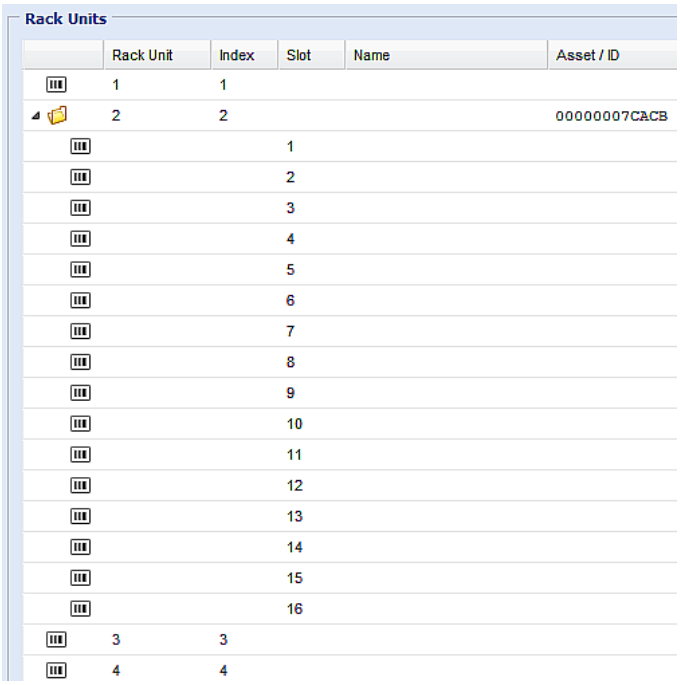
So erweitern Sie den Ordner für einen Blade-Erweiterungsstrip:

1. Klicken Sie im linken Fensterbereich auf den gewünschten Assetsensor. Die Seite des ausgewählten Assetsensors wird im rechten Fensterbereich geöffnet.

2. Suchen Sie die Rackeinheit (Tag-Port), an die der Blade-Erweiterungsstrip angeschlossen ist.



3. Doppelklicken Sie auf die Rackeinheit, oder klicken Sie auf den weißen Pfeil ▷ vor dem Ordnersymbol. Der Pfeil wird anschließend als schwarz abfallender Pfeil ◢ dargestellt, und alle Tag-Ports werden unter dem Ordner angezeigt.



So blenden Sie einen Blade-Erweiterungsstrip aus:

- Doppelklicken Sie auf den Ordner des Blade-Erweiterungsstrips, oder klicken Sie auf den schwarzen, abfallenden Pfeil ◢ vor dem Ordnersymbol. Alle Tag-Ports unter dem Ordner werden ausgeblendet.

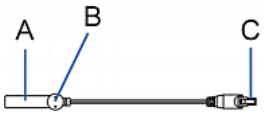
Anschließen von Blade-Erweiterungsstrips

Bei Blade-Servern, die in einem einzigen Gehäuse untergebracht sind, können Sie einzelne Blade-Server über einen Blade-Erweiterungsstrip verfolgen.

Der Blade-Erweiterungsstrip von Raritan funktioniert ähnlich dem Raritan-Assetsensor, benötigt aber ein Tag-Anschlusskabel für den Anschluss an einen Tag-Port am regulären Assetsensor oder AMS-M2-Z. Der Blade-Erweiterungsstrip enthält je nach Modell 4 bis 16 Tag-Ports.

Die Abbildung zeigt ein Tag-Anschlusskabel und einen Blade-Erweiterungsstrip mit 16 Tag-Ports.

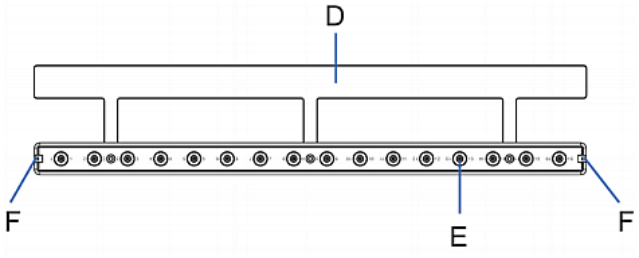
Tag-Anschlusskabel



Position	Beschreibung
A	Strichcode (ID-Nummer) für das Tag-Anschlusskabel
B	Tag-Stecker
C	Kabelanschluss zum Anschließen des Blade-Erweiterungsstrips

Hinweis: Ein Tag-Anschlusskabel hat einen eindeutigen Strichcode. Dieser wird in der EMX-Webschnittstelle zur Identifikation jedes Blade-Erweiterungsstrips angezeigt, an den es angeschlossen ist.

Blade-Erweiterungsstrip



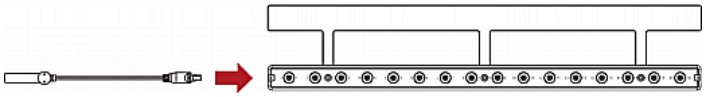
Position	Beschreibung
D	Mylar-Bereich mit Klebeband
E	Tag-Ports

Position	Beschreibung
F	Kabelbuchse(n) zum Anschließen des Tag-Anschlusskabels

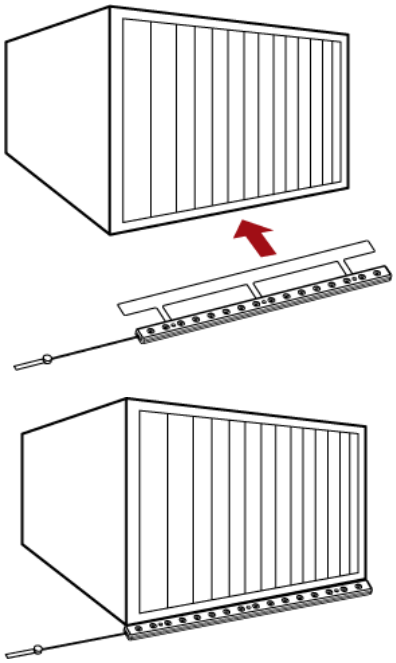
Hinweis: Jeder Tag-Port auf dem Blade-Erweiterungsstrip ist mit einer Nummer versehen, die als Slot-Nummer in der EMX-Webschnittstelle angezeigt wird.

So installieren Sie einen Blade-Erweiterungsstrip:

1. Schließen Sie das Tag-Anschlusskabel an den Blade-Erweiterungsstrip an.
   - Stecken Sie den Stecker des Kabels in eine der beiden Buchsen des Blade-Erweiterungsstrips.



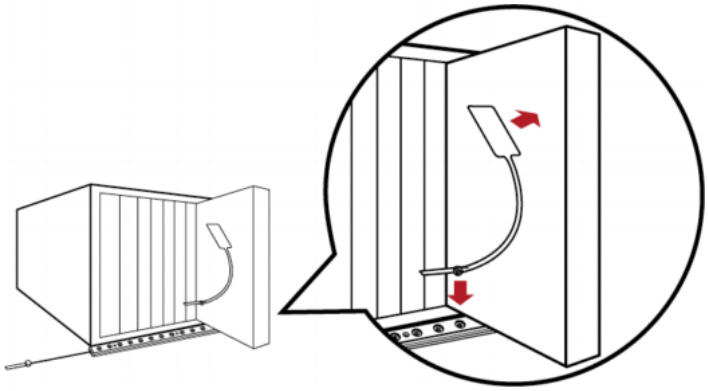
2. Schieben Sie den Blade-Erweiterungsstrip unter das Blade-Gehäuse, bis sich der Mylar-Bereich vollständig unter dem Gehäuse befindet. Vergewissern Sie sich, dass sich der Blade-Erweiterungsstrip nicht löst. Verwenden Sie ggf. das Klebeband an der Rückseite des Mylar-Bereichs, um den Strip zu fixieren.



3. Schließen Sie ein Ende des Asset-Tags an den Blade-Server und das andere Ende an den Blade-Erweiterungsstrip an.

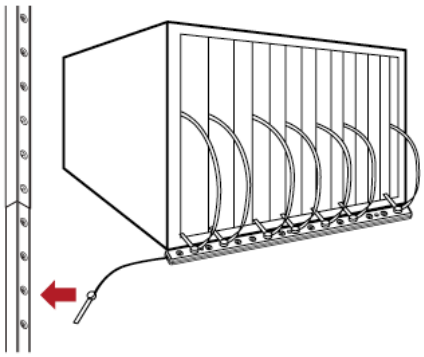
a. Befestigen Sie das Asset-Tag mit dem Klebeband des Tags an einer Seite des Blade-Servers.

b. Schließen Sie den Tag-Stecker des Asset-Tags am Tag-Port des Blade-Erweiterungsstrips an.



4. Wiederholen Sie den vorhergehenden Schritt, bis alle Blade-Server im Gehäuse über die Asset-Tags mit dem Blade-Erweiterungsstrip verbunden sind.

5. Schließen Sie den Tag-Stecker des Blade-Erweiterungsstrips am nächstgelegenen Tag-Port der Assetsensor-Baugruppe oder des AMS-M2-Z-Assetsensors am Rack an.



Hinweis: Wenn Sie den Tag-Stecker des Blade-Erweiterungsstrips vorübergehend abziehen müssen, warten Sie mindestens 1 Sekunde, bevor Sie ihn wieder anschließen, weil die EMX-Einheit ihn sonst nicht erkennt.

Webcams

Die EMX-Einheit unterstützt Logitech® QuickCam® Pro 9000 Webcams, die daran angeschlossen sind, sodass Sie Video- oder Momentaufnahmen des Bereichs um die Webcam ansehen können. Das EMX 888-Gerät unterstützt bis zu zwei (2) Webcams, und das EMX 111-Gerät unterstützt eine (1) Webcam. Nachdem eine Webcam angeschlossen wurde, können Sie die Umgebungsbedingungen in der Nähe der EMX-Einheit von einem beliebigen Standort aus über die Webschnittstelle visuell überwachen.

Weitere Informationen zur QuickCam-Webcam finden Sie in der mitgelieferten Benutzerdokumentation. Informationen zum Anschließen einer Webcam an die EMX-Einheit finden Sie unter ***Anschluss einer Logitech-Webcam (optional)*** (auf Seite 39).

Von der Webcam aufgezeichnete Momentaufnahmen oder Videos werden im rechten Fensterbereich der EMX-Webschnittstelle angezeigt, wenn eine Webcam in der Navigationsstruktur ausgewählt ist. Momentaufnahmen und Videos lassen sich auch im Live-Vorschaumodus im Fenster "Primary Standalone Live Preview" (Primäre eigenständige Live-Vorschau) anzeigen, indem Sie auf das Symbol für die Live-Vorschau klicken.

EMX bietet Ihnen die Möglichkeit, Momentaufnahmen von jeder Webcam zu erfassen und zu speichern. Weitere Informationen finden Sie unter ***Erfassen, Anzeigen und Verwalten von Webcam-Momentaufnahmen*** (auf Seite 205).

Links zu Videos, die mit einer Webcam aufgezeichnet wurden, können über E-Mail oder Sofortnachrichten gesendet werden. Siehe ***Senden von Videos in einer E-Mail oder Sofortnachricht*** (auf Seite 207).

Es können Ereignisse erstellt werden, die E-Mails mit Momentaufnahmen einer Webcam auslösen. Sie können für jede einzelne Webcam Ereignisse definieren. Siehe ***Ereignisregeln und Aktionen*** (auf Seite 137).Um Webcams konfigurieren zu können, muss Ihrer Funktion die Berechtigung zum Ändern der Webcam-Konfiguration zugewiesen sein. Sie benötigen zudem die Berechtigung zum Anzeigen von Webcam-Bildern und Konfiguration, um Bilder in EMX anzeigen zu können.

Konfigurieren von Webcams

Bevor Sie eine Webcam konfigurieren können, müssen Sie sie an die EMX-Einheit anschließen. Siehe ***Anschluss einer Logitech-Webcam (optional)*** (auf Seite 39).

So konfigurieren Sie eine Webcam:

1. Klicken Sie in der Navigationsstruktur auf den Ordner "Webcam Management" (Webcam-Verwaltung). Die Seite "Webcam Management" (Webcam-Verwaltung) wird geöffnet.
2. Klicken Sie auf die Webcam, die Sie konfigurieren möchten, und dann auf "Setup" (Einrichten) unten rechts auf der Seite. Das Dialogfeld "Webcam Setup" (Webcam einrichten) wird geöffnet.
3. Geben Sie einen Namen für die Webcam ein. Es werden bis zu 64 Zeichen unterstützt.
4. Wählen Sie eine Auflösung für die Webcam aus.
5. Wählen Sie den Webcam-Modus aus. Dieser kann nach Bedarf geändert werden, nachdem die Webcam konfiguriert wurde.
   a. Video – die Webcam ist im Videomodus. Legen Sie die Bildwiederholfrequenz (Bilder pro Sekunde) fest.
   b. Snapshot (Momentaufnahme) – die Webcam zeigt Bilder der Webcam. Legen Sie für "Time Between Image(s)" (Zeit zwischen Bilder(n)) die Zeit in Sekunden fest.
6. Klicken Sie auf OK. Das von der Webcam aufgezeichnete Bild oder Video ist jetzt in der EMX-Einheit verfügbar, wenn Sie in der Navigationsstruktur auf die Webcam klicken.

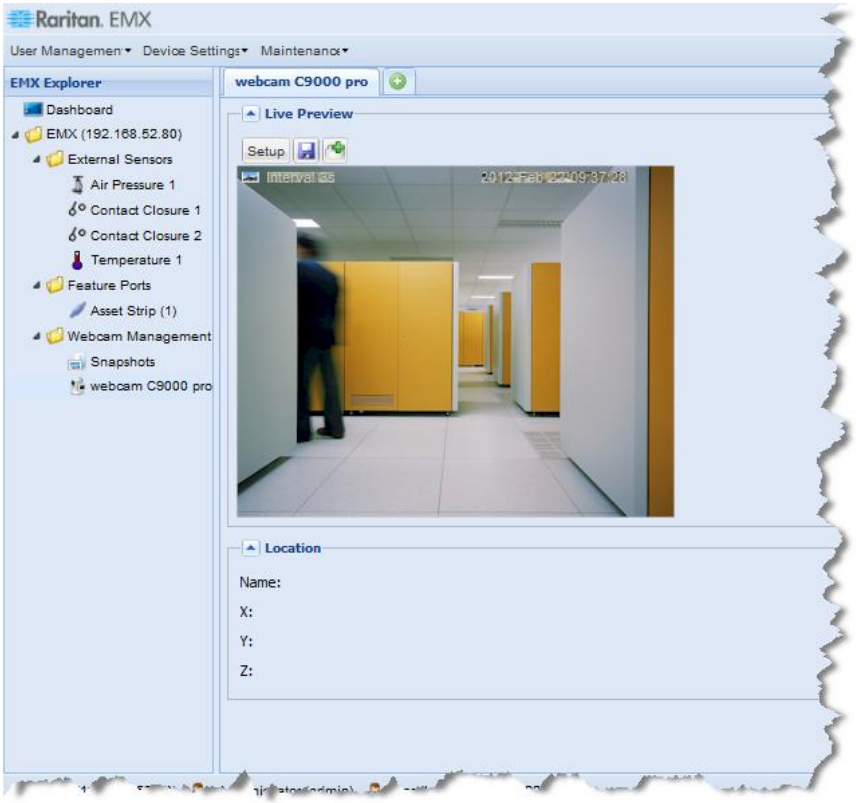
So bearbeiten Sie eine Webcam-Konfiguration:

1. Klicken Sie in der Navigationsstruktur auf den Ordner "Webcam Management" (Webcam-Verwaltung). Die Seite "Webcam Management" (Webcam-Verwaltung) wird geöffnet.
2. Doppelklicken Sie auf die Webcam, die Sie bearbeiten möchten. Das Webcam-Bild oder -Video wird auf einer neuen Registerkarte geöffnet.
3. Klicken Sie auf "Setup" (Einrichten).
4. Bearbeiten Sie die Informationen nach Bedarf. Änderungen an der Auflösung gelten nicht für bestehende, gespeicherte Bilder, nur für Bilder und Videos, die nach einer Änderung der Auflösung aufgenommen wurden.
5. Klicken Sie auf OK.

Anzeigen von Webcam-Momentaufnahmen und -Videos

Nachdem eine Webcam angeschlossen wurde, ist sie standardmäßig darauf eingestellt, dass sie alle fünf (5) Sekunden eine Momentaufnahme macht. Ändern Sie die Webcam-Einstellungen und/oder wechseln Sie zwischen Momentaufnahmen und Live-Video, indem Sie das Dialogfeld "Webcam Setup" (Webcam einrichten) aufrufen. Klicken Sie dazu in der Navigationsstruktur auf eine Webcam und dann im Fensterbereich "Live Preview" (Live-Vorschau) auf die Schaltfläche "Setup" (Einrichten). Siehe ***Konfigurieren von Webcams*** (auf Seite 203).

Von einer Webcam aufgezeichnete Momentaufnahmen oder Videos werden im rechten Fensterbereich der EMX-Webschnittstelle angezeigt, wenn eine Webcam in der Navigationsstruktur ausgewählt wird.



Im Momentaufnahmen-Modus wird oben links im Bild ein entsprechendes Symbol sowie die Anzahl der Bilder angezeigt, die die Webcam pro Sekunde aufnimmt. Im Videomodus wird ein entsprechendes Symbol oben links im Bild angezeigt. Um zwischen dem Momentaufnahmen- und Videomodus zu wechseln, klicken Sie auf "Setup" (Einrichten) und wählen das Optionsfeld "Image" (Bild) oder "Video" aus.

Auf jeder Momentaufnahme wird außerdem das Datum und die Uhrzeit angezeigt. Der Standort der Webcam wird im Fensterbereich "Location" (Standort) unter dem Bild angezeigt, zusammen mit Kennzeichnungen, die der Webcam zugewiesen wurden. Siehe ***Konfigurieren von Webcams*** (auf Seite 203).

In der EMX-Schnittstelle können gleichzeitig bis zu fünf (5) Live-Vorschausitzungen auf verschiedenen Registerkarten oder in separaten Live-Vorschaufenstern angezeigt werden. Um darauf zuzugreifen, klicken Sie über der Momentaufnahme bzw. dem Video auf das Symbol .

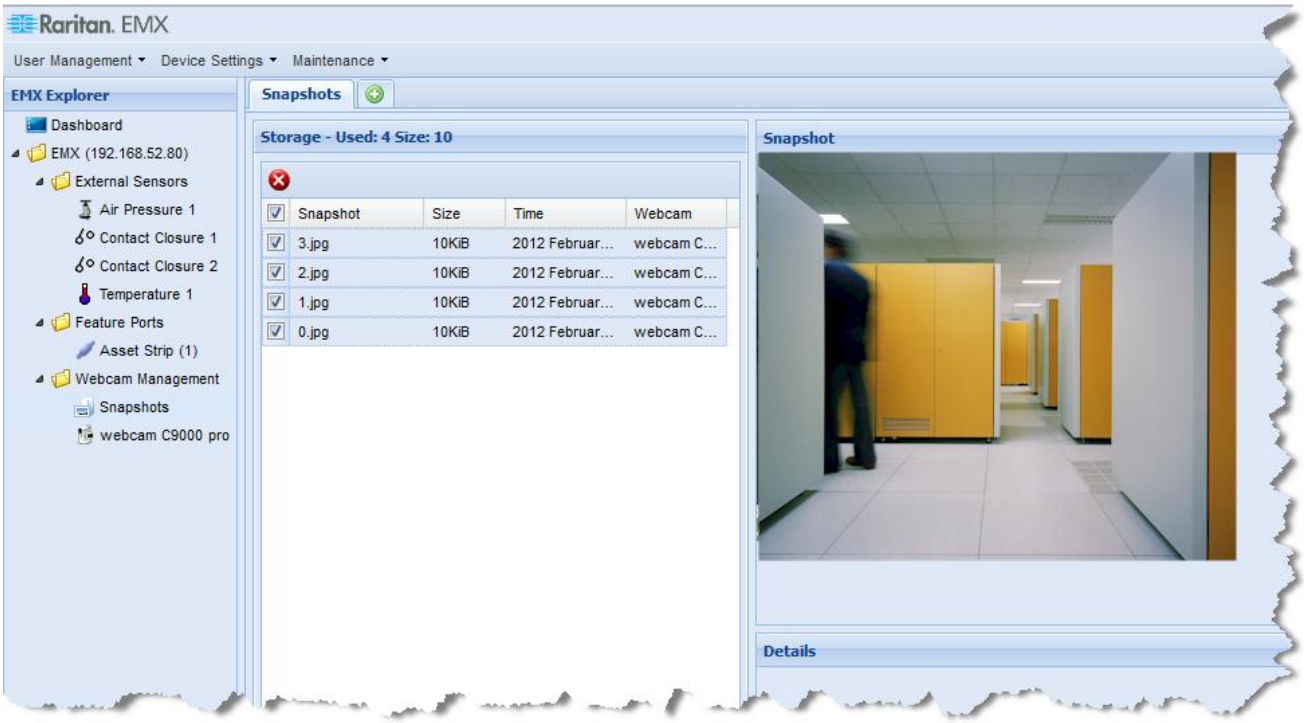
Hinweis: Bei fernen Live-Vorschausitzungen, z. B. den Sitzungen, auf die über einen Link in einer E-Mail oder einer Sofortnachricht zugegriffen wird, werden maximal (3) Live-Vorschausitzungen gleichzeitig unterstützt. Eine (1) vom Absender in der EMX-Schnittstelle und bis zu zwei (2) Remote-Sitzungen.

Einzelne, von einer Webcam erfasste Momentaufnahmen lassen sich durch Klicken auf "Snapshots" (Momentaufnahmen) unter "Webcam Management" (Webcam-Verwaltung) in der Navigationsstruktur anzeigen. Nach der Auswahl wird die Registerkarte "Snapshots" (Momentaufnahmen) im rechten Fensterbereich geöffnet. Weitere Informationen finden Sie unter ***Erfassen, Anzeigen und Verwalten von Webcam-Momentaufnahmen*** (auf Seite 205) und Anzeigen und Verwalten gespeicherter Momentaufnahmen.

Erfassen, Anzeigen und Verwalten von Webcam-Momentaufnahmen

Nachdem Sie eine Momentaufnahme mit der Funktion "Store Snapshot to Webcam Storage" (Momentaufnahme in Webcam-Speicher ablegen) aufgezeichnet haben, wird diese auf der EMX-Einheit gespeichert. Auf der EMX-Einheit lassen sich bis zu zehn (10) Bilder gleichzeitig speichern. Sofern Sie Momentaufnahmen nicht manuell löschen, wird die älteste Momentaufnahme automatisch gelöscht, wenn die Anzahl der Momentaufnahmen zehn Aufnahmen übersteigt.

Dateien für Momentaufnahmen werden als JPG-Dateien gespeichert. Der Name einer solchen Datei basiert auf der Nummer der Momentaufnahme, wobei mit 1 begonnen wird. Folglich lautet der Name der ersten erfassten Momentaufnahme 1.jpg, der Name der zweiten Aufnahme 2.jpg usw.



So machen Sie eine Momentaufnahme von einer Webcam:

1. Klicken Sie in der Navigationsstruktur auf die Webcam, mit der Sie eine Momentaufnahme machen möchten. Das Webcam-Bild wird im rechten Fensterbereich angezeigt.

   Die Webcam muss sich im Momentaufnahmen-Modus befinden, um Momentaufnahmen aufzeichnen zu können. Wenn sich die Webcam im Videomodus befindet, klicken Sie im rechten Fensterbereich über dem Videobild auf "Setup" (Einrichten), um das Dialogfeld "Webcam Setup" (Webcam einrichten) zu öffnen. Wählen Sie anschließend das Optionsfeld "Snapshot" (Momentaufnahme) aus.

2. Wenn die von der ausgewählten Webcam zu erfassende Momentaufnahme im rechten Fensterbereich angezeigt wird, klicken Sie über dem Bild auf das Symbol , um eine Momentaufnahme zu machen. Auf dem Gerät lassen sich bis zu zehn (10) Momentaufnahmen gleichzeitig speichern.

So zeigen Sie vorhandene Momentaufnahmen an:

1. Klicken Sie in der Navigationsstruktur unter dem Ordner "Webcam Management" (Webcam-Verwaltung) auf "Snapshot" (Momentaufnahme). Die Momentaufnahmen werden im rechten Fensterbereich im Abschnitt "Storage" (Speicher) angezeigt.

2. Um eine einzelne Momentaufnahme anzuzeigen, klicken Sie im Bereich "Storage" (Speicher) der Seite auf die Datei für die Momentaufnahme.

   Beim Anzeigen von Momentaufnahmen werden die Größe jeder Datei, das Datum und die Uhrzeit der Aufnahme und die Webcam angezeigt, mit der die einzelnen Momentaufnahmen gemacht wurden.

   Details, z. B. der Webcam-Standort und/oder Kennungen, sofern vorhanden, werden im Bereich "Details" unter der Momentaufnahme im rechten Fensterbereich angezeigt. Diese Informationen werden bei der Erstkonfiguration der Webcam definiert. Siehe ***Konfigurieren von Webcams*** (auf Seite 203).

So löschen Sie Momentaufnahmen von Hand:

- Löschen Sie Momentaufnahmen, indem Sie das Kontrollkästchen neben der zu löschenden Momentaufnahme aktivieren und auf das Löschen-Symbol oben im Bereich klicken. Um alle Momentaufnahmen gleichzeitig auszuwählen und zu löschen, klicken Sie auf das Kontrollkästchen im Spaltenkopf und dann auf das Löschen-Symbol.

Senden von Videos in einer E-Mail oder Sofortnachricht

Sie können einen Link zu Webcams, die an die EMX-Einheit angeschlossen sind, per E-Mail oder Sofortnachricht an bis zu zwei (2) Empfänger senden. Benutzer können anschließend auf die Links klicken und Momentaufnahmen oder Videos ansehen.

Hinweis: Bei fernen Live-Vorschausitzungen, z. B. den Sitzungen, auf die über einen Link in einer E-Mail oder einer Sofortnachricht zugegriffen wird, werden maximal (3) Live-Vorschausitzungen gleichzeitig unterstützt. Eine (1) vom Absender in der EMX-Schnittstelle und bis zu zwei (2) Remote-Sitzungen.

Hinweis: In diesem Abschnitt ist Benutzer A der Absender der Nachricht und Benutzer B der Empfänger der Nachricht.

Der Empfänger kann über den Link auf das Videobild zugreifen, solange entweder:

- das Video im Live-Vorschaumodus der EMX-Schnittstelle von Benutzer A geöffnet ist und Benutzer A sich nicht von der Schnittstelle abmeldet und die Sitzung das Zeitlimit nicht überschreitet.

  Oder

- das Video in einem zweiten Live-Vorschaufenster in der EMX-Schnittstelle von Benutzer A geöffnet bleibt. Solange das zweite Live-Vorschaufenster in der Schnittstelle von Benutzer A geöffnet ist, ist der Link auch dann verfügbar, wenn sich Benutzer A von der EMX-Schnittstelle abmeldet oder die Sitzung das Zeitlimit überschreitet.

Bewährte Vorgehensweise

Benutzer A sollte das Video in der EMX-Schnittstelle in einem zweiten Live-Vorschaufenster öffnen und dieses Fenster mindestens so lange geöffnet lassen, bis Benutzer B das Video über den Link öffnet.

Sobald Benutzer B das Video über den Link öffnet, kann das zweite Live-Vorschaufenster in der EMX-Schnittstelle von Benutzer A geschlossen werden.

Benutzer B muss Benutzer A manuell mitteilen, dass er den Link geöffnet hat, oder Benutzer A kann prüfen, ob Benutzer B derzeit an mit der Anwendung verbunden ist, indem er auf "Maintenance" > "Connected Users" (Wartung > Angeschlossene Benutzer) klickt.

So senden Sie einen Video-Link per E-Mail oder Sofortnachricht:

1. Klicken Sie in der Navigationsstruktur auf die Webcam, die das Video aufnimmt, für das Sie einen Link in der E-Mail bereitstellen möchten. Das Video wird in der Live-Vorschau im rechten Fensterbereich angezeigt.
2. Klicken Sie auf das Symbol oberhalb des Videos. Das Video wird in einem zweiten Live-Vorschaufenster geöffnet.
3. Kopieren Sie die URL aus dem Live-Vorschaufenster in die E-Mail oder die Anwendung für die Sofortnachricht. Lassen Sie das Live-Vorschaufenster mindestens so lange geöffnet, bis der Empfänger das Video über den Link öffnet.

GSM-Modems

Um SMS-Ereignisnachrichten senden zu können, muss ein Cinterion® GSM-Modem vom Typ MC52i/MC55i an die EMX-Einheit angeschlossen sein. Weitere Informationen zu SMS-Ereignisnachrichten finden Sie unter ***Erstellen von Aktionen*** (auf Seite 143).

Hinweis: Die EMX-Einheit kann keine SMS-Nachrichten empfangen.

So schließen Sie das GSM-Modem an:

1. Schließen Sie das GSM-Modem an den seriellen DB9-Port der EMX-Einheit an.

2. Konfigurieren Sie das GSM-Modem nach Bedarf. Informationen zum Konfigurieren des GSM-Modems finden Sie in der Hilfe zum Modem.

Schroff LHX-Wärmetauscher

Nachdem Sie den Schroff® LHX-Wärmetauscher über den Feature-Port oder den RS-485-Port an das EMX-Gerät angeschlossen haben, erkennt die EMX-Einheit den LHX. Je nachdem, an welchen Port der LHX angeschlossen ist, wird er in der Navigationsstruktur unter dem Ordner "Feature" oder "Auxiliary Port" (Zusätzlicher Port) angezeigt.

Hinweis: Wenn Sie den LHX an den Feature-Port anschließen, verwenden Sie das serielle Kabel, das mit dem LHX geliefert wurde.

Über die EMX-Einheit können Sie folgende Aufgaben per Fernzugriff ausführen:

- Benennen eines angeschlossenen LHX-Wärmetauschers
- Konfigurieren des Sollwerts für die Luftaustrittstemperatur
- Konfigurieren der Schwellenwerte für die Luftaustrittstemperatur
- Konfigurieren der Schwellenwerte für die Lufteintrittstemperatur
- Konfigurieren der Schwellenwerte für die Wassereintrittstemperatur
- Konfigurieren der Schwellenwerte für die Lüfterdrehzahl
- Überwachen der Lufteintrittstemperatur
- Überwachen der Luftaustrittstemperatur
- Überwachen der Lüfterdrehzahl
- Konfigurieren der Basiseinstellungen für den angeschlossenen Wärmetauscher, z. B. die Sensorschwellenwerte

Hinweis: Diese Einstellungen werden auf dem EMX-Port gespeichert, an dem der Wärmetauscher angeschlossen ist. Sie gehen verloren, wenn der Wärmetauscher an einen anderen Port angeschlossen wird.

Informationen zum Anschließen des Wärmetauschers finden Sie unter ***Anschluss eines Schroff LHX-Wärmetauschers (optional)*** (auf Seite 40).

Aktivieren und Deaktivieren der Unterstützung für Schroff LHX-Wärmetauscher

Die Unterstützung für Schroff LHX-Wärmetauscher ist standardmäßig deaktiviert. Die Unterstützung muss als solche aktiviert werden, bevor das Gerät in der Navigationsstruktur oder dem Dashboard angezeigt wird. Außerdem muss die Unterstützung für den Schroff LHX-Wärmetauscher aktiviert sein, damit über SNMP auf die LHX-MIB zugegriffen werden kann.

So aktivieren Sie den Schroff LHX-Wärmetauscher:

1. Wählen Sie "Device Settings" > "Features" (Geräteeinstellungen > Features), und aktivieren Sie im Menü das Kontrollkästchen "Schroff Heat Exchanger" (Schroff-Wärmetauscher).
2. Klicken Sie zur Bestätigung auf "Yes" (Ja).
3. Starten Sie das EMX-Gerät neu.

Benennen eines Wärmetauschers

Weisen Sie einem LHX-Wärmetauscher einen Namen zu, um den Wärmetauscher in der EMX-Webschnittstelle identifizieren zu können. Hinter dem angepassten Namen des LHX-Wärmetauschers stehen der Gerätetyp und die RS-485-Port-Nummer in Klammern.

Die Webschnittstelle bietet zwei Arten von Einrichtungsdialogfeldern zum Benennen eines bestimmten LHX-Wärmetauschers.

So weisen Sie einem Wärmetauscher mithilfe des Dialogfelds "Auxiliary Port Setup" (Zusätzlichen Port einrichten) einen Namen zu:

1. Falls noch nicht geschehen, schließen Sie den LHX-Wärmetauscher an die EMX-Einheit an.
2. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*
3. Klicken Sie auf den Ordner "Auxiliary Ports" (Zusätzliche Ports). Die Seite "Auxiliary Ports" (Zusätzliche Ports) wird im rechten Fensterbereich mit einer Liste aller RS-485-Ports geöffnet.

4. Wählen Sie den Port, an den der gewünschte Wärmetauscher angeschlossen ist, auf der Seite "Auxiliary Ports" (Zusätzliche Ports) aus, und klicken Sie auf "Setup" (Einrichtung). Sie können auch auf den Port doppelklicken. Das Dialogfeld "Auxiliary Ports Setup" (Zusätzliche Ports einrichten) für den ausgewählten Port wird angezeigt.
5. Geben Sie im Feld "Name" einen Namen für den Wärmetauscher ein.
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

So weisen Sie einem Wärmetauscher mithilfe des entsprechenden Einrichtungsdialogfelds einen Namen zu:

1. Erweitern Sie den Ordner "Auxiliary Ports" (Zusätzliche Ports), wenn er nicht erweitert ist, um alle an die RS-485-Ports angeschlossenen Geräte anzuzeigen.
2. Klicken Sie im Fenster "EMX Explorer" auf den gewünschten Wärmetauscher. Die für diesen Wärmetauscher spezifische Seite wird im rechten Fensterbereich geöffnet.
3. Klicken Sie im Bereich "Settings" (Einstellungen) auf "Setup" (Einrichtung).
4. Geben Sie im Feld "Name" einen Namen für den Wärmetauscher ein.
5. Klicken Sie auf "OK", um die Änderungen zu speichern.

Konfigurieren von Temperatur- und Lüfterschwellenwerten

Ein LHX-Wärmetauscher wird mit verschiedenen Sensoren zur Ermittlung der Lufttemperatur, der Wassertemperatur und der Lüfterdrehzahl implementiert. Sie können Schwellenwerte für diese Sensoren einrichten, sodass Sie vom EMX-Gerät benachrichtigt werden, wenn sich die Sensorergebnisse einer kritischen Bedingung nähern. Diese Einstellungen werden auf dem EMX-Port gespeichert, an dem der Wärmetauscher angeschlossen ist. Sie gehen verloren, wenn der Wärmetauscher an einen anderen Port angeschlossen wird.

So konfigurieren Sie die Schwellenwerte für einen Sensor:

1. Falls noch nicht geschehen, schließen Sie den LHX-Wärmetauscher an die EMX-Einheit an.
2. Erweitern Sie den Ordner "Auxiliary Ports" (Zusätzliche Ports), wenn er nicht erweitert ist, um alle an die RS-485-Ports angeschlossenen Geräte anzuzeigen.
3. Klicken Sie im Fenster "EMX Explorer" auf den gewünschten Wärmetauscher. Die für diesen Wärmetauscher spezifische Seite wird im rechten Fensterbereich geöffnet.

4. Wählen Sie den gewünschten Sensor in der Tabelle "Sensors" (Sensoren) aus, und klicken Sie auf "Setup Thresholds" (Schwellenwerte einrichten), oder doppelklicken Sie einfach auf den Sensor. Für den ausgewählten Sensor wird ein Einrichtungsdialogfeld angezeigt.
5. Passen Sie die Einstellungen für die Schwellenwerte und die Deassertionshysterese an. Wenn die in den Feldern "Upper Critical" (Oberer kritischer Schwellenwert) und "Lower Critical" (Unterer kritischer Schwellenwert) definierten Schwellenwerte erreicht werden, stuft die EMX-Einheit die Umgebungsbedingungen als kritisch und außerhalb des akzeptablen Bereichs ein.
   - Zum Aktivieren eines Schwellenwerts aktivieren Sie das entsprechende Kontrollkästchen. Zum Deaktivieren eines Schwellenwerts deaktivieren Sie das Kontrollkästchen.
   - Nachdem Sie einen Schwellenwert aktiviert haben, geben Sie den entsprechenden numerischen Wert in das dazugehörige Textfeld ein.
   - Um die Deassertionshysterese für alle Schwellenwerte zu aktivieren, geben Sie einen numerischen Wert ungleich Null in das Feld "Deassertion Hysteresis" (Deassertionshysterese) ein. Siehe ***Was ist Deassertionshysterese?*** (auf Seite 189)
6. Klicken Sie auf "OK", um die Änderungen zu speichern.

Überwachen des Wärmetauschers

Mit der EMX-Webschnittstelle können Sie den Status jedes angeschlossenen LHX-Wärmetauschers sowie den Status jedes integrierten LHX-Sensors überwachen.

Anzeigen der Übersicht

Auf den Seiten "Dashboard" und "Auxiliary Ports" (Zusätzliche Ports) wird eine Übersicht aller angeschlossenen LHX-Wärmetauscher angezeigt, einschließlich der Nummer des RS-485-Ports, an den jeder Wärmetauscher angeschlossen ist, sowie des Status jedes Wärmetauschers.

Ein in der Übersicht rot hervorgehobener LHX-Wärmetauscher weist auf einen LHX-Sensorfehler am Wärmetauscher hin. Sehen Sie sich die Spalte "State" (Zustand) oder "Status" an, um die ausgefallenen Sensoren zu identifizieren.

So zeigen Sie die LHX-Übersicht auf der Seite "Dashboard" an:

1. Klicken Sie im Fenster "EMX Explorer" auf das Dashboard-Symbol. Die Seite "Dashboard" wird im rechten Fensterbereich geöffnet.

2. Suchen Sie den Bereich "LHX Heat Exchanger" (LHX-Wärmetauscher), in dem eine Liste der angeschlossenen LHX-Wärmetauscher angezeigt wird.

So zeigen Sie die LHX-Übersicht auf der Seite "Auxiliary Ports" (Zusätzliche Ports) an:

1. Wenn der Ordner "EMX" nicht erweitert ist, erweitern Sie diesen, um alle Komponenten anzuzeigen.

   Hinweis: Der EMX-Folder heißt standardmäßig "EMX". Der Name ändert sich nach dem Anpassen des Gerätenamens. Siehe **Benennen des EMX-Geräts** *(auf Seite 74).*

2. Klicken Sie auf den Ordner "Auxiliary Ports" (Zusätzliche Ports). Die Seite "Auxiliary Ports" (Zusätzliche Ports) wird im rechten Fensterbereich mit einer Liste aller RS-485-Ports geöffnet.

Anzeigen von Details

Auf einer Seite für LHX-Wärmetauscher werden detaillierte Informationen angezeigt, darunter:

- Geräteinformationen und -einstellungen, z. B. die Nummer des RS-485-Ports und der Gerätename
- Die Luftaustrittstemperatur
- Ergebnisse und Zustände aller integrierten LHX-Sensoren
- Kumulierte Betriebsstunden
- Fehler, z. B. ausgefallene LHX-Sensoren oder Aktivierung der Notkühlung

So zeigen Sie Details eines bestimmten LHX-Wärmetauschers an:

1. Erweitern Sie den Ordner "Auxiliary Ports" (Zusätzliche Ports), wenn er nicht erweitert ist, um alle an die RS-485-Ports angeschlossenen Geräte anzuzeigen.

   Klicken Sie im Fenster "EMX Explorer" auf den gewünschten Wärmetauscher. Die für diesen Wärmetauscher spezifische Seite wird im rechten Fensterbereich geöffnet.

Wenn ein LHX-Sensorergebnis den kritischen oder den Warnschwellenwert erreicht oder über- bzw. unterschreitet, wird die entsprechende Zeile mit dem Sensorergebnis gelb oder rot dargestellt. Siehe ***Gelb oder Rot hervorgehobene Ergebnisse*** (auf Seite 58).

Gerätestatus und Symbolwechsel

Die EMX-Webschnittstelle ändert Symbole, um verschiedene Zustände jedes angeschlossenen LHX-Wärmetauschers darzustellen.

Symbol	Gerätestatus
	Der Wärmetauscher ist eingeschaltet und arbeitet normal.
	Der Wärmetauscher ist ausgeschaltet.
	Der Wärmetauscher ist eingeschaltet, wechselt aber aufgrund eines LHX-Sensorfehlers in den kritischen Zustand.
	Mindestens ein LHX-Sensorergebnis hat den oberen oder unteren Warnschwellenwert über- oder unterschritten.
	An diesem RS-485-Port wurde KEIN Gerät erkannt.

Sehen Sie sich Folgendes an, um die Ursache des kritischen Zustands festzustellen:

- Den Bereich "LHX Heat Exchanger" (LHX-Wärmetauscher) auf der Seite "Dashboard". Siehe ***Überwachen des Wärmetauschers*** (auf Seite 212).
- Die Seite "Auxiliary Ports" (Zusätzliche Ports). Siehe ***Überwachen des Wärmetauschers*** (auf Seite 212).
- Den Bereich "Alert States" (Alarmstatus) auf der Seite des LHX-Wärmetauschers. Siehe ***Alarmstatus und LHX-Ereignisprotokoll*** (auf Seite 214).

Alarmstatus und LHX-Ereignisprotokoll

Wenn ein LHX-Wärmetauscher physisch an das EMX-Gerät angeschlossen ist, wird auf der entsprechenden Geräteseite der Bereich "Alert States" (Alarmstatus) angezeigt. Der Bereich "Alert States" (Alarmstatus) zeigt Informationen an, die die derzeit ausgefallenen LHX-Sensoren kennzeichnen.

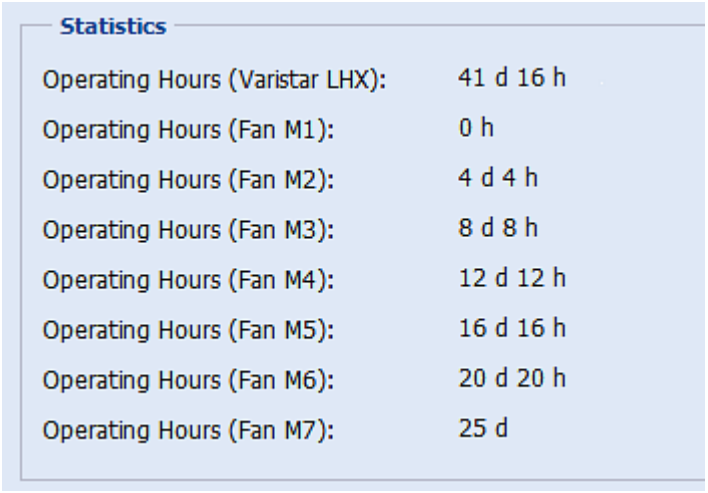
Tipp: Die Seiten "Dashboard" und "Auxiliary Ports" (Zusätzliche Ports) weisen ebenfalls auf ausgefallene Sensoren hin. Siehe **Überwachen des Wärmetauschers** *(auf Seite 212).*

Die Schaltfläche "Show Event Log" (Ereignisprotokoll anzeigen) befindet sich im Bereich "Alert States" (Alarmstatus). Klicken Sie auf diese Schaltfläche, um die Ereignisse anzuzeigen, die mit dem EMX-Gerät verbunden sind.

Betriebsstunden

Betriebsstunden sind die kumulierte Zeit seit dem ersten Anschließen des LHX-Wärmetauschers an das EMX-Gerät und dem Einschalten des Wärmetauschers.

Die EMX-Webschnittstelle zeigt die Betriebsstunden für den Wärmetauscher und seine Lüfter. Informationen zu den Betriebsstunden finden Sie im Bereich "Statistics" (Statistik) auf den Seiten für Wärmetauscher.


Statistics
Operating Hours (Varistar LHX): 41 d 16 h
Operating Hours (Fan M1): 0 h
Operating Hours (Fan M2): 4 d 4 h
Operating Hours (Fan M3): 8 d 8 h
Operating Hours (Fan M4): 12 d 12 h
Operating Hours (Fan M5): 16 d 16 h
Operating Hours (Fan M6): 20 d 20 h
Operating Hours (Fan M7): 25 d

Unten sind die Zeiteinheiten aufgeführt, die für Betriebsstunden verwendet werden:

- h: Stunde(n)
- d: Tag(e)

"3d 5h" bedeutet z. B., dass die Gesamtbetriebszeit 3 Tage und 5 Stunden beträgt.

Steuern des Wärmetauschers

Das EMX-Gerät bietet Ihnen die Möglichkeit, einen angeschlossenen Wärmetauscher per Fernzugriff ein- oder auszuschalten.

So steuern Sie den LHX-Wärmetauscher:

1. Erweitern Sie den Ordner "Auxiliary Ports" (Zusätzliche Ports), wenn er nicht erweitert ist, um alle an die RS-485-Ports angeschlossenen Geräte anzuzeigen.

   Klicken Sie im Fenster "EMX Explorer" auf den gewünschten Wärmetauscher. Die für diesen Wärmetauscher spezifische Seite wird im rechten Fensterbereich geöffnet.

2. Suchen Sie den Bereich "Information".

- Um den LHX-Wärmetauscher auszuschalten, klicken Sie auf "Switch Off" (Ausschalten).
- Um den LHX-Wärmetauscher einzuschalten, klicken Sie auf "Switch On" (Einschalten).

3. Wenn Sie im vorhergehenden Schritt auf "Switch Off" (Ausschalten) geklickt haben, müssen Sie den Vorgang bestätigen. Klicken Sie auf "Yes" (Ja), um ihn auszuschalten, oder auf "No" (Nein), um den Vorgang abzubrechen.

Das in der Webschnittstelle angezeigte Symbol des Wärmetauschers wird nach dem Ein- oder Ausschalten geändert. Siehe ***Gerätestatus und Symbolwechsel*** (auf Seite 214).

Kapitel 9 Verwenden von SNMP

In diesem Abschnitt über SNMP wird die Einrichtung der EMX-Einheit für die Verwendung mit einem SNMP-Manager beschrieben. Die EMX-Einheit kann für das Senden von Traps an einen SNMP-Manager und den Empfang von GET- und SET-Befehlen konfiguriert werden, um den Status abzurufen und einige grundlegende Einstellungen vorzunehmen.

In diesem Kapitel

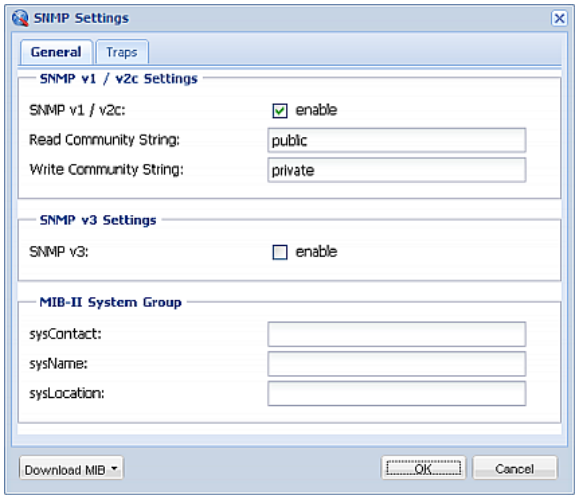
Aktivieren von SNMP.....217
Konfigurieren der Benutzer für die verschlüsselte SNMP-V3-Kommunikation.....218
Konfigurieren von SNMP-Traps.....219
SNMP-GET- und SET-Befehle.....220

Aktivieren von SNMP

Zur Kommunikation mit einem SNMP-Manager müssen Sie auf dem EMX-Gerät zunächst den SNMP-Agenten aktivieren.

So aktivieren Sie SNMP:

1. Wählen Sie "Device Settings" > "Network Services" > "SNMP" (Geräteeinstellungen > Netzwerkdienste > SNMP) aus. Das Dialogfeld "SNMP Settings" (SNMP-Einstellungen) wird angezeigt.



2. Wählen Sie das Kontrollkästchen "enable" (aktivieren) im Feld "SNMP v1 / v2c", um die Kommunikation mit einem SNMP-Manager über das SNMP-v1 oder -v2c-Protokoll zu aktivieren.

- Geben Sie im Feld "Read Community String" (Lese-Community-String) den SNMP-Lese-Community-String ein. Dieser String ist normalerweise "public" (öffentlich).
- Geben Sie im Feld "Write Community String" (Schreib-Community-String) den Lese-/Schreib-Community-String ein. Dieser String ist normalerweise "private" (privat).

3. Wählen Sie das Kontrollkästchen "enable" (aktivieren) im Feld "SNMP v3", um die Kommunikation mit einem SNMP-Manager über das SNMP-V3-Protokoll zu aktivieren.

Tipp: Sie können einem Benutzer den Zugriff auf die EMX-Einheit über das SNMP-V3-Protokoll gewähren oder verweigern. Siehe **Konfigurieren der Benutzer für die verschlüsselte SNMP-V3-Kommunikation** *(auf Seite 218).*

4. Geben Sie im Feld "sysContact" (Systemkontakt) den "sysContact"-Wert der SNMP-MIB-II ein.
5. Geben Sie im Feld "sysName" (Systemname) den "sysName"-Wert der SNMP-MIB-II ein.
6. Geben Sie im Feld "sysLocation" (Systemstandort) den "sysLocation"-Wert der SNMP-MIB-II ein.
7. Klicken Sie auf "OK", um die Änderungen zu speichern.

Wichtig: Sie müssen die SNMP-MIB für EMX herunterladen, um dies mit SNMP-Manager zu verwenden. Klicken Sie auf "Download MIB" (MIB herunterladen) in diesem Dialogfeld, um die gewünschte MIB-Datei herunterzuladen. Weitere Informationen finden Sie unter *Herunterladen einer SNMP-MIB* (auf Seite 220).

Konfigurieren der Benutzer für die verschlüsselte SNMP-V3-Kommunikation

Das SNMP-V3-Protokoll ermöglicht eine verschlüsselte Kommunikation. Zur Nutzung dieser Funktion müssen Benutzer über einen Authentifizierungsschlüssel (Authentication Pass Phrase) und Privatschlüssel (Privacy Pass Phrase) verfügen, die als geheimer Schlüssel zwischen ihnen und der EMX-Einheit dienen.

So konfigurieren Sie Benutzer für die verschlüsselte SNMP-V3-Kommunikation:

1. Wählen Sie "User Management" > "Users" (Benutzerverwaltung > Benutzer) aus. Das Dialogfeld "Manage Users" (Benutzer verwalten) wird angezeigt.
2. Wählen Sie den Benutzer aus, indem Sie auf ihn klicken.

3. Klicken Sie auf "Edit" (Bearbeiten), oder doppelklicken Sie auf den Benutzer. Das Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) wird angezeigt, wobei XXX den Benutzernamen darstellt.
4. Um die Zugriffsberechtigungen von SNMPv3 zu ändern, klicken Sie auf die Registerkarte "SNMPv3" und nehmen die erforderlichen Änderungen vor. Weitere Einzelheiten finden Sie unter ***Erstellen von Benutzerprofilen*** (auf Seite 62) in Schritt 6.
5. Klicken Sie auf "OK", um die Änderungen zu speichern. Der Benutzer ist nun für die verschlüsselte SNMP-V3-Kommunikation konfiguriert.

Konfigurieren von SNMP-Traps

Die EMX-Einheit führt automatisch ein internes Protokoll über die stattfindenden Ereignisse. Siehe ***Konfigurieren von Ereignisregeln*** (siehe "***Ereignisregeln und Aktionen***" auf Seite 137). Diese Ereignisse können zum Senden von SNMP-Traps an einen externen Manager verwendet werden.

So konfigurieren Sie die EMX-Einheit für das Senden von SNMP-Traps:

1. Wählen Sie "Device Settings" > "Event Rules" (Geräteeinstellungen > Ereignisregeln) aus. Das Fenster "Event Rule Settings" (Ereignisregeleinstellungen) wird eingeblendet.
2. Wählen Sie auf der Registerkarte "Rules" (Regeln) die Option "System SNMP Trap Rule" (System-SNMP-Trap-Regel).
3. Klicken Sie auf das Kontrollkästchen "Enabled" (Aktiviert), um diese Ereignisregel zu aktivieren.
4. Klicken Sie auf "Save" (Speichern), um die Änderungen zu speichern.
5. Klicken Sie auf die Registerkarte "Actions" (Aktionen), wenn Sie keine SNMP-Trap-Aktionen konfiguriert haben.
6. Wählen Sie "System SNMP Trap Action" (System-SNMP-Trap-Aktion), um die Trap-Ziele einzurichten.
7. Geben Sie im Feld "Host 1" eine IP-Adresse ein. Hierbei handelt es sich um die IP-Adresse, an die der SNMP-Agent Traps sendet.
8. Geben Sie im Feld "Port 1" die Nummer für den Kommunikationsport ein.
9. Geben Sie im Feld "Community" den Namen der SNMP-Community ein. Die Community ist die Gruppe, der die EMX-Einheit und alle SNMP-Verwaltungsstationen angehören.
10. Um mehr als ein SNMP-Trap-Ziel anzugeben, wiederholen Sie Schritt 8 bis 10 für weitere Ziele. Es können maximal 3 Ziele angegeben werden.

11. Klicken Sie auf "Save" (Speichern), um die Änderungen zu speichern.
12. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Hinweis: Wenn Sie EMX auf eine neue Version aktualisieren, müssen Sie die vom SNMP-Manager verwendete MIB auch aktualisieren. Damit wird sichergestellt, dass für den SNMP-Manager die korrekte MIB zur Verfügung steht. Siehe **Herunterladen einer SNMP-MIB** *(auf Seite 220).*

SNMP-GET- und SET-Befehle

Neben dem Senden von Traps kann die EMX-Einheit SNMP-GET- und -SET-Befehle von externen SNMP-Managern empfangen.

- GET-Befehle werden verwendet, um Informationen zum EMX-Gerät (z. B. den Systemstandort) abzurufen.
- Mit SET-Befehlen wird ein Teil dieser Informationen (z. B. der SNMP-Systemname) konfiguriert.

  Hinweis: Der SNMP-Systemname entspricht dem Namen des EMX-Geräts. Wenn Sie den SNMP-Systemnamen ändern, ändert sich auch der in der Webschnittstelle angezeigte Gerätename.

  Das EMX-Gerät bietet KEINE Unterstützung für die Konfiguration von IPv6-Parametern mit SNMP-SET-Befehlen.

Für diese Befehle können nur die Objekte der SNMP-MIB-II-Systemgruppe und der benutzerdefinierten EMX-MIB verwendet werden.

Die EMX-MIB

Die SNMP-MIB-Datei ist zur Verwendung Ihres EMX-Geräts mit einem SNMP-Manager erforderlich. SNMP-MIB-Dateien beschreiben die SNMP-Funktionen.

Herunterladen einer SNMP-MIB

Sie SNMP-MIB-Datei für die EMX-Einheit kann über die Webschnittstelle leicht heruntergeladen werden. Es gibt zwei Möglichkeiten, die SNMP-MIB-Datei herunterzuladen.

So laden Sie die Datei über das Dialogfeld "SNMP Settings" (SNMP-Einstellungen) herunter:

1. Wählen Sie "Device Settings" > "Network Services" > "SNMP" (Geräteeinstellungen > Netzwerkdienste > SNMP) aus. Das Dialogfeld "SNMP Settings" (SNMP-Einstellungen) wird angezeigt.

2. Klicken Sie auf "Download MIB" (MIB herunterladen). Es wird ein Untermenü mit den MIB-Dateien angezeigt.
3. Wählen Sie die gewünschte MIB-Datei zum Herunterladen aus.
   - EMD-MIB: Die SNMP-MIB-Datei zum Verwalten des EMX-Geräts.
   - ASSETMANAGEMENT-MIB: Die SNMP-MIB-Datei für das Asset-Management.
   - LHX-MIB: Die SNMP-MIB-Datei zum Verwalten des/der LHX-Wärmetauscher(s).

   Hinweis: Die Unterstützung für den Schroff LHX muss aktiviert sein, damit die LHX-MIB verfügbar ist. Siehe **Aktivieren und Deaktivieren der Unterstützung für Schroff LHX-Wärmetauscher** *(auf Seite 210).*
4. Klicken Sie auf "Save" (Speichern), um die Datei auf Ihrem Computer zu speichern.

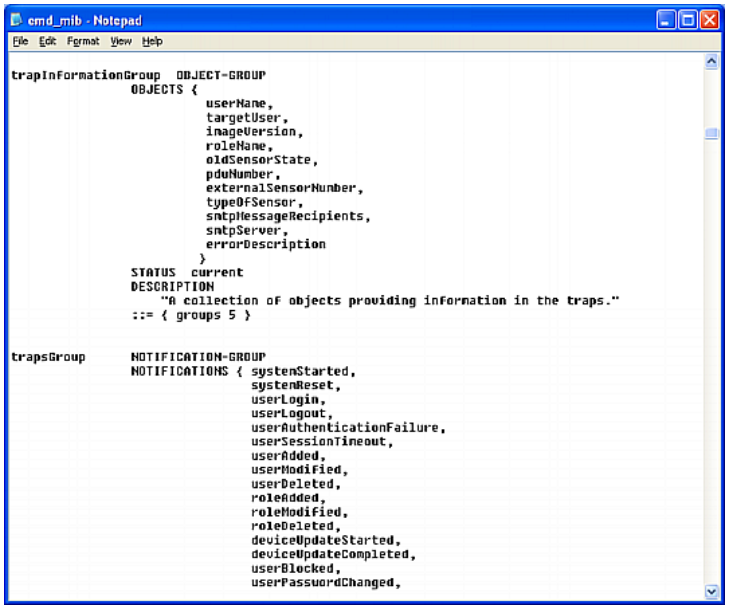
So laden Sie die Datei über das Dialogfeld "Device Information" (Geräteinformationen) herunter:

1. Wählen Sie "Maintenance" > "Device Information" (Wartung > Geräteinformationen) aus. Das Dialogfeld "Device Information" (Geräteinformationen) wird eingeblendet.
2. Klicken Sie auf den "Download"-Link im Feld EMD-MIB, ASSETMANAGEMENT-MIB oder LHX-MIB, um die gewünschte SNMP-MIB-Datei herunterzuladen.
3. Klicken Sie auf "Save" (Speichern), um die Datei auf Ihrem Computer zu speichern.

Layout

Wenn Sie die MIB öffnen, werden die benutzerdefinierten Objekte angezeigt, die das EMX-System beschreiben.

Standardmäßig werden diese Objekte zunächst am Anfang der Datei unter der übergeordneten Gruppe aufgelistet. Anschließend folgt eine individuelle Auflistung, in der jedes Objekt detailliert definiert und beschrieben ist.



Die Gruppe "measurementsGroup" enthält z. B. Objekte für Umgebungssensoren, die an das EMX-Gerät angeschlossen sind. Ein unter dieser Gruppe aufgeführtes Objekt, measurementsExternalSensorState, wird später in der MIB als Sensorstatus beschrieben. boardFirmwareVersion, das Teil der Gruppe "configGroup" ist, beschreibt die Firmwareversion.

SNMP-SET-Befehle und Schwellenwerte

Einige Objekte können im SNMP-Manager mit SNMP-SET-Befehlen konfiguriert werden. Für konfigurierbare Objekte ist in der MIB die Lese-/Schreibberechtigung MAX-ACCESS (MAX. ZUGRIFF) festgelegt.

Zu diesen Objekten gehören Schwellenwertobjekte, die dazu führen, dass die EMX-Einheit eine Warnung ausgibt und ein SNMP-Trap sendet, wenn bestimmte Parameter über- bzw. unterschritten werden. Siehe ***Schwellenwertinformationen*** (auf Seite 189), um eine Beschreibung der Funktionsweise von Schwellenwerten zu erhalten.

Hinweis: Wenn Sie die Schwellenwerte über SNMP-SET-Befehle konfigurieren, stellen Sie sicher, dass der Wert des oberen kritischen Schwellenwerts höher ist als die obere Warngrenze.

Kapitel 10 Verwenden der Befehlszeilenschnittstelle

In diesem Kapitel

Informationen zur Schnittstelle 224
Anmelden bei der CLI 225
Befehl "help" 228
Anzeigen von Informationen 228
Konfigurieren von EMX-Gerät und Netzwerk 240
Aufheben der Sperrung eines Benutzers 331
Zurücksetzen der EMX-Einheit 332
Behebung von Netzwerkproblemen 333
Abfragen verfügbarer Parameter für einen Befehl 337
Abrufen vorheriger Befehle 337
Automatisches Vervollständigen eines Befehls 337
Abmelden bei der CLI 338
Wiederherstellen der werksseitigen Standardeinstellungen (CLI) 338

Informationen zur Schnittstelle

Die EMX-Einheit stellt eine Befehlszeilenschnittstelle bereit, über die Administratoren von Rechenzentren einige grundlegende Verwaltungsaufgaben ausführen können.

Mit dieser Schnittstelle können Sie folgende Aufgaben ausführen:

- EMX-Gerät zurücksetzen
- Anzeigen der EMX- und Netzwerkinformationen, wie z. B. Gerätename, Firmwareversion, IP-Adresse usw.
- Konfigurieren der EMX und Netzwerkeinstellungen
- Beheben von Netzwerkproblemen

Sie können die Schnittstelle über eine serielle Verbindung mit einem Terminalemulationsprogramm (z. B. HyperTerminal) oder über einen Telnet- oder SSH-Client (z. B. PuTTY).

Hinweis: Der Telnet-Zugriff ist standardmäßig deaktiviert, weil die Kommunikation offen stattfindet und daher nicht sicher ist. Informationen zum Aktivieren von Telnet finden Sie unter **Ändern der Netzwerkdiensteinstellungen** *(auf Seite 89).*

Anmelden bei der CLI

Die Anmeldung über HyperTerminal und eine lokale Verbindung unterscheidet sich geringfügig von der Anmeldung über SSH oder Telnet.

Mit HyperTerminal

Sie können beliebige Terminalemulationsprogramme für den lokalen Zugriff auf die Befehlszeilenschnittstelle verwenden.

In diesem Abschnitt wird HyperTerminal beschrieben, das Teil des Windows-Betriebssystem von Windows Vista ist.

So melden Sie sich über HyperTerminal an:

1. Schließen Sie einen Computer über eine lokale Verbindung an das EMX-Gerät an.
2. Starten Sie HyperTerminal auf dem Computer, und öffnen Sie ein Konsolenfenster. Das Fenster ist anfangs leer.

   Stellen Sie sicher, dass die Einstellungen des COM-Ports die folgende Konfiguration verwenden:

   - Bits per second (Bits pro Sekunde) = 115200 (115,2 Kbit/s)
   - Data bits (Datenbits) = 8
   - Stop bits (Stoppbits) = 1
   - Parity (Parität) = None (Keine)
   - Flow control (Flusssteuerung) = None (Keine)

   Tipp: Bei einer USB-Verbindung können Sie feststellen, welcher COM-Port der EMX-Einheit zugeordnet ist. Wählen Sie dazu "Control Panel" (Systemsteuerung) > "System" > "Hardware" > "Device Manager" (Geräte-Manager)", und suchen Sie "Dominion Serial Console" (Serielle Dominion-Konsole) in der Gruppe "Ports".

3. Drücken Sie die Eingabetaste. Die Eingabeaufforderung für den Benutzernamen wird angezeigt.

   ```
   Username: _
   ```

4. Geben Sie einen Namen ein, und drücken Sie die Eingabetaste. Beim Namen ist die Groß-/Kleinschreibung zu beachten. Anschließend werden Sie zur Eingabe eines Kennworts aufgefordert.

```
Username: admin
Password: _
```

5. Geben Sie ein Kennwort ein und drücken Sie die Eingabetaste. Beim Kennwort ist die Groß-/Kleinschreibung zu beachten.

   Nachdem Sie das Kennwort richtig eingegeben haben, wird die Systemaufforderung # oder > angezeigt. Weitere Einzelheiten finden Sie unter ***Unterschiedliche CLI-Modi und -Eingabeaufforderungen*** (auf Seite 227).

   Tipp: Die Information "Last Login" (Letzte Anmeldung), einschließlich Datum und Uhrzeit, wird auch angezeigt, wenn das selbe Benutzerprofil einmal zur Anmeldung bei der EMX-Webschnittstelle oder -CLI verwendet wurde.

6. Jetzt sind Sie bei der Befehlszeilenschnittstelle angemeldet und können mit der Verwaltung des EMX-Geräts beginnen.

Mit SSH oder Telnet

Sie können sich extern bei der Befehlszeilenschnittselle anmelden. Hierfür verwenden Sie einen SSH- oder Telnet-Client, wie z. B. PuTTY.

Hinweis: PuTTY ist ein kostenloses Programm, das im Internet zum Download angeboten wird. Einzelheiten zur Konfiguration von PuTTY finden Sie in der Dokumentation des Programms.

So melden Sie sich über SSH oder Telnet an:

1. Vergewissern Sie sich, dass SSH oder Telnet aktiviert wurde. Siehe ***Ändern der Netzwerkdiensteinstellungen*** (auf Seite 89).
2. Starten Sie einen SSH- oder Telnet-Client, und öffnen Sie ein Konsolenfenster. Eine Anmeldeaufforderung wird eingeblendet.

```
login as:
```

3. Geben Sie einen Namen ein, und drücken Sie die Eingabetaste. Beim Namen ist die Groß-/Kleinschreibung zu beachten.

   Hinweis: Wenn Sie den SSH-Client verwenden, darf der Name NICHT länger als 25 Zeichen sein. Andernfalls tritt ein Fehler bei der Anmeldung auf.

   Anschließend werden Sie zur Eingabe eines Kennworts aufgefordert.

```
login as: admin
admin@192.168.84.88's password:
```

4. Geben Sie ein Kennwort ein und drücken Sie die Eingabetaste. Beim Kennwort ist die Groß-/Kleinschreibung zu beachten.
5. Nachdem Sie das Kennwort richtig eingegeben haben, wird die Systemaufforderung # oder > angezeigt. Weitere Einzelheiten finden Sie unter ***Unterschiedliche CLI-Modi und -Eingabeaufforderungen*** (auf Seite 227).

   Tipp: Die Information "Last Login" (Letzte Anmeldung), einschließlich Datum und Uhrzeit, wird auch angezeigt, wenn das selbe Benutzerprofil einmal zur Anmeldung bei der EMX-Webschnittstelle oder -CLI verwendet wurde.
6. Jetzt sind Sie bei der Befehlszeilenschnittstelle angemeldet und können mit der Verwaltung des EMX-Geräts beginnen.

Unterschiedliche CLI-Modi und -Eingabeaufforderungen

Je nach verwendetem Anmeldename und aufgerufenem Modus ist die Systemeingabeaufforderung in der CLI unterschiedlich.

- User Mode (Benutzermodus): Wenn Sie sich als normaler Benutzer ohne uneingeschränkte Berechtigung zur Konfiguration des EMX-Geräts anmelden, wird die Eingabeaufforderung **>** angezeigt.
- Administrator Mode (Administratormodus): Wenn Sie sich als Administrator mit uneingeschränkter Berechtigung zur Konfiguration des EMX-Geräts anmelden, wird die Eingabeaufforderung # angezeigt.
- Configuration Mode (Konfigurationsmodus): Über den Administratormodus können Sie den Konfigurationsmodus aufrufen. In diesem Modus ändert sich die Eingabeaufforderung in **config:#**, und Sie können die Konfiguration von EMX-Gerät und Netzwerk ändern. Siehe ***Aufrufen des Konfigurationsmodus*** (auf Seite 240).
- Diagnostic Mode (Diagnosemodus): Über den Administratormodus können Sie den Diagnosemodus aufrufen. In diesem Modus ändert sich die Eingabeaufforderung in **diag:>**, und Sie können Befehle zur Behebung von Netzwerkfehlern ausführen, wie z. B. den Befehl "ping". Siehe ***Aufrufen des Diagnosemodus*** (auf Seite 333).

Schließen einer seriellen Verbindung

Schließen Sie das Fenster oder Terminalemulationsprogramm, wenn Sie nicht mehr über die serielle Verbindung auf ein EMX-Gerät zugreifen möchten.

Wenn Sie auf EMX-Geräte zugreifen oder mehrere davon aktualisieren, wechseln Sie nicht das serielle Kabel von Gerät zu Gerät, ohne vorher das Fenster für die serielle Verbindung zu schließen.

Befehl "help"

Der Befehl "help" zeigt eine Liste der wichtigsten CLI-Befehle an. Dies kann hilfreich sein, wenn Sie mit den Befehlen nicht vertraut sind.

Die Syntax für den Befehl "help" lautet:

```
#      help
```

Drücken Sie nach Eingabe des Befehls die Eingabetaste, daraufhin wird eine Liste mit den wichtigsten Befehlen angezeigt.

Tipp: Sie können prüfen, welche Parameter für einen bestimmten CLI-Befehl zur Verfügung stehen, indem Sie am Ende des Befehls ein Fragezeichen anfügen. Siehe **Abfragen verfügbarer Parameter für einen Befehl** *(auf Seite 337).*

Anzeigen von Informationen

Sie können die Anzeigebefehle verwenden, um die aktuellen Einstellungen oder den Status des EMX-Geräts oder einen Teil davon anzuzeigen, z. B. IP-Adresse, Netzwerkmodus, Firmwareversion usw.

Einige "show"-Befehle (Anzeigebefehle) haben zwei Formate: eines mit dem Parameter "details" und eines ohne. Der Unterschied besteht darin, dass der Befehl ohne den Parameter "details" eine verkürzte Version der Informationen anzeigt, während der andere detaillierte Informationen anzeigt.

Nach Eingabe eines "show"-Befehls (Anzeigebefehl) drücken Sie zu dessen Ausführung die Eingabetaste.

Hinweis: Abhängig von Ihrem Anmeldenamen kann die Eingabeaufforderung # durch die Eingabeaufforderung > ersetzt werden.

Netzwerkkonfiguration

Dieser Befehl zeigt die gesamte Netzwerkkonfiguration an, wie z. B. IP-Adresse, Netzwerkmodus und MAC-Adresse.

```
#        show network
```

IP-Konfiguration

Dieser Befehl zeigt nur die IP-Konfiguration an, z. B. IPv4- und IPv6-Konfiguration, Adresse(n), Gateway und Subnetzmaske.

```
#        show network ip <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *all*, *v4* oder *v6*.

Option	Beschreibung
all	Diese Option zeigt die IPv4- und die IPv6-Einstellungen. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
v4	Diese Option zeigt nur die IPv4-Einstellungen.
v6	Diese Option zeigt nur die IPv6-Einstellungen.

LAN-Schnittstelleneinstellungen

Dieser Befehl zeigt nur die LAN-Schnittstelleninformationen, z. B. Geschwindigkeit der LAN-Schnittstelle, Duplexmodus und aktueller LAN-Schnittstellenstatus.

```
#        show network interface
```

Netzwerkmodus

Dieser Befehl zeigt an, ob es sich beim aktuellen Netzwerkmodus um einen drahtgebundenen oder drahtlosen Netzwerkmodus handelt.

```
#        show network mode
```

Drahtloskonfiguration

Dieser Befehl zeigt nur die Drahtloskonfiguration des EMX-Geräts, z. B. den SSID-Parameter.

```
#        show network wireless
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show network wireless details
```

Netzwerkdiensteinstellungen

Dieser Befehl zeigt nur die Netzwerkdiensteinstellungen, einschließlich der Telnet-Einstellung, der TCP-Ports für HTTP-, HTTPS- und SSH-Dienste sowie der SNMP-Einstellungen.

```
#        show network services <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *all*, *http*, *https*, *telnet*, *ssh*, *snmp* und *zeroconfig*.

Option	Beschreibung
all	Zeigt die Einstellungen aller Netzwerkdienste an, einschließlich HTTP, HTTPS, Telnet, SSH und SNMP. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
http	Zeigt nur den TCP-Port für den HTTP-Dienst an.
https	Zeigt nur den TCP-Port für den HTTPS-Dienst an.
telnet	Zeigt nur die Einstellungen des Telnet-Diensts an.
ssh	Zeigt nur die Einstellungen des SSH-Diensts an.
snmp	Zeigt nur die SNMP-Einstellungen an.
zeroconfig	Zeigt nur die Einstellungen der konfigurationslosen Bekanntmachung an.

Einstellungen von Assetsensoren

Dieser Befehl zeigt die Einstellungen von Assetsensoren an, z. B. die Gesamtanzahl der Rackeinheiten (Tag-Ports), den Status des Assetsensors, den Nummerierungsmodus, die Ausrichtung, die verfügbaren Tags und die Einstellungen für die LED-Farbe.

```
#        show assetStrip <n>
```

Variablen:

- <n> ist eine der folgenden Optionen: *all* (alle) oder eine Zahl.

Option	Beschreibung
all	Zeigt alle Informationen zu Assetsensoren an. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
Eine bestimmte Nummer eines Assetsensors	Zeigt die Einstellungen des Assetsensors an, der an die angegebene FEATURE-Port-Nummer angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die gültige Nummer immer 1.

Diese Befehlssyntax legt die LED-Farbe für alle Rackeinheiten an den angeschlossenen Assetsensoren fest, um das Fehlen eines angeschlossenen Asset-Tag anzugeben.

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variablen:

- <color> ist der hexadezimale RGB-Wert einer Farbe im HTML-Format. Die <color>-Variable liegt zwischen #000000 und #FFFFFF.

Informationen zum Umgebungssensor

Diese Befehlssyntax zeigt die Informationen zum angegebenen Umgebungssensor an.

```
#        show sensor externalsensor <n>
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show sensor externalsensor <n> details
```

Variablen:

- <n> ist die Nummer des Umgebungssensors. Die Nummer des Umgebungssensors ist die ID, die dem Sensor zugewiesen wurde und die auf der Seite "External Sensors" (Externer Sensoren) der EMX-Webschnittstelle angezeigt wird.

Angezeigte Informationen:

- Ohne den Parameter "details" (Details) werden nur die Einstellungen für Messergebnis, Schwellenwert, Deassertion-Hysterese und Assertionszeitlimit für den angegebenen Umgebungssensor angezeigt.
- Mithilfe des Parameters "details" werden zusätzliche Sensorinformationen angezeigt, einschließlich Genauigkeit und Bereich.

Hinweis: Bei einem Einzelsensor (ein/aus) sind die Daten zu Schwellenwert und Genauigkeit NICHT verfügbar.

Informationen zum Umgebungssensor

Diese Befehlssyntax zeigt die Informationen zum Umgebungssensor an.

```
#        show externalsensors <n>
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show externalsensors <n> details
```

Variablen:

- <n> ist eine der folgenden Optionen: *all* (alle) oder eine Zahl.

Option	Beschreibung
all	Zeigt die Informationen für alle Umgebungssensoren an. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
Eine bestimmte Umgebungssensor-Nummer*	Zeigt nur Informationen für den angegebenen Umgebungssensor an.

* Die Nummer des Umgebungssensors ist die ID, die dem Sensor zugewiesen wurde und die auf der Seite "External Sensors" (Externer Sensoren) der EMX-Webschnittstelle angezeigt wird.

Angezeigte Informationen:

- Ohne den Parameter "details" werden nur die Sensor-ID, der Sensortyp und der Messwert angezeigt.

  Hinweis: Einzelsensoren (Ein/Aus-Sensoren) zeigen den Sensorstatus anstelle des Messwerts an.

- Mit dem Parameter "details" werden neben der ID und dem Sensormesswert weitere Informationen angezeigt, wie z. B. Seriennummer sowie X-, Y- und Z-Koordinaten.

Schwellenwertinformationen zum Umgebungssensor

Diese Befehlssyntax zeigt die Schwellenwertinformationen zum angegebenen Umgebungssensor an.

```
#        show sensor externalsensor <n>
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show sensor externalsensor <n> details
```

Variablen:

- <n> ist die Nummer des Umgebungssensors. Die Nummer des Umgebungssensors ist die ID, die dem Sensor zugewiesen wurde und die auf der Seite "External Sensors" (Externer Sensoren) der EMX-Webschnittstelle angezeigt wird.

Angezeigte Informationen:

- Ohne den Parameter "details" (Details) werden nur die Einstellungen für Messergebnis, Schwellenwert, Deassertion-Hysterese und Assertionszeitlimit für den angegebenen Umgebungssensor angezeigt.
- Mithilfe des Parameters "details" werden zusätzliche Sensorinformationen angezeigt, einschließlich Genauigkeit und Bereich.

Hinweis: Bei einem Einzelsensor (ein/aus) sind die Daten zu Schwellenwert und Genauigkeit NICHT verfügbar.

Security Settings (Sicherheitseinstellungen)

Dieser Befehl zeigt die Sicherheitseinstellungen des EMX-Geräts an.

```
#        show security
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show security details
```

Angezeigte Informationen:

- Ohne den Parameter "details" werden Informationen wie die IP-Zugriffssteuerung, die rollenbasierte Zugriffssteuerung, die Kennwortrichtlinie und die HTTPS-Verschlüsselung angezeigt.
- Mit dem Parameter "details" werden weitere Sicherheitsinformationen angezeigt wie die Dauer der Benutzersperrung und das Zeitlimit bei Inaktivität des Benutzers.

Bestehende Benutzerprofile

Dieser Befehl zeigt die Daten eines oder aller bestehenden Benutzerprofile.

```
#        show user <user_name>
```

Um detaillierte Informationen anzuzeigen, fügen Sie den Parameter "details" am Ende des Befehls ein.

```
#        show user <user_name> details
```

Variablen:

- <user_name> ist der Name des Benutzers, dessen Profil Sie abfragen möchten. Für die Variable kann eine der folgenden Optionen angegeben werden: *all* oder der Name eines Benutzers.

Option	Beschreibung
all	Diese Option zeigt alle bestehenden Benutzerprofile an. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*

Option	Beschreibung
Name eines bestimmten Benutzers	Diese Option zeigt nur das Profil des angegebenen Benutzers an.

Angezeigte Informationen:

- Ohne den Parameter "details" werden nur vier Benutzerinformationen angezeigt: Benutzername, Status "enabled" (aktiviert), SNMP-v3-Zugriffsberechtigung und Benutzerfunktion(en).
- Mit dem Parameter "details" werden weitere Benutzerinformationen angezeigt, z. B. Telefonnummer, E-Mail-Adresse, bevorzugte Temperatureinheit usw.

Bestehende Benutzerfunktionen

Dieser Befehl zeigt die Daten eines oder aller bestehenden Benutzerfunktionen.

```
#       show roles <role_name>
```

Variablen:

- <role_name> ist der Name der Benutzerfunktion, dessen Berechtigungen Sie abfragen möchten. Für die Variable kann eine der folgenden Optionen angegeben werden:

Option	Beschreibung
all	Diese Option zeigt alle bestehenden Benutzerfunktionen an. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
Name einer bestimmten Benutzerfunktion	Diese Option zeigt nur die Daten der angegebenen Benutzerfunktion.

Angezeigte Informationen:

- Die Einstellungen für die Benutzerfunktion werden angezeigt, einschließlich der Funktionsbeschreibung und der Berechtigungen.

Einstellungen von Rackeinheiten eines Assetsensors

Bei einem Raritan-Assetsensor bezieht sich eine Rackeinheit auf einen Tag-Port. Dieser Befehl zeigt die Einstellungen einer bestimmten Rackeinheit oder aller Rackeinheiten an einem Assetsensor an, z. B. die LED-Farbe und den LED-Modus einer Rackeinheit.

```
#        show rackUnit <n> <rack_unit>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist eine der folgenden Optionen: *all* oder die Indexnummer einer bestimmten Rackeinheit.

Option	Beschreibung
all	Zeigt die Einstellungen aller Rackeinheiten am angegebenen Assetsensor an. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
Eine bestimmte Nummer	Zeigt die Einstellungen der angegebenen Rackeinheit am angegebenen Assetsensor an. Geben Sie die Rackeinheit mithilfe der Indexnummer an. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.

Einstellungen für einen Blade-Erweiterungsstrip

Dieser Befehl zeigt die Informationen eines Blade-Erweiterungsstrips an, einschließlich der Gesamtanzahl der Tag-Ports, und, sofern verfügbar, die ID (den Strichcode) angeschlossener Tags.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist die Indexnummer der gewünschten Rackeinheit (Tag-Port) am ausgewählten Assetsensor. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.
- <blade_slot> ist eine der folgenden Optionen: *all* oder eine bestimme Nummer eines Tag-Ports am Blade-Erweiterungsstrip.

Option	Beschreibung
all	Zeigt die Informationen aller Tag-Ports am angegebenen Blade-Erweiterungsstrip an, der an eine bestimmte Rackeinheit angeschlossen ist. *Tipp: Sie können auch den Befehl eingeben, ohne diese Option "all" hinzuzufügen, um die selben Daten zu erhalten.*
Eine bestimmte Nummer	Zeigt die Informationen des angegebenen Tag-Ports am Blade-Erweiterungsstrip an, der an eine bestimmte Rackeinheit angeschlossen ist. Die Nummern der einzelnen Tag-Ports am Blade-Erweiterungsstrip sind auf der Seite "Asset Strip" verfügbar.

Befehlsverlauf

Diese Befehlssyntax zeigt den Befehlsverlauf für die aktuelle Verbindungssitzung an.

```
#       show history
```

Angezeigte Informationen:

- Eine Liste der zuvor in der aktuellen Sitzung eingegebenen Befehle wird angezeigt.

Größe des Verlaufspuffers

Diese Befehlssyntax zeigt die Größe des Verlaufspuffers zum Speichern der Verlaufsbefehle an.

```
#       show history bufferlength
```

Angezeigte Informationen:

- Die aktuelle Größe des Verlaufspuffers wird angezeigt.

Beispiele

Dieser Abschnitt zeigt Beispiele für den Befehl "show".

Beispiel 1 – Allgemeine Sicherheitsinformationen

Dieses Diagramm zeigt die Ausgabe des Befehls *show security* an.

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Beispiel 2 – Detaillierte Sicherheitsinformationen

Wenn der Befehl *show security details* eingegeben wird, werden weitere Informationen angezeigt.

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Konfigurieren von EMX-Gerät und Netzwerk

Für die Konfiguration des EMX-Geräts oder der Netzwerkeinstellungen über die CLI müssen Sie sich als Administrator anmelden.

Aufrufen des Konfigurationsmodus

Sie müssen den Konfigurationsmodus aufrufen, da die Konfigurationsbefehle nur im Konfigurationsmodus funktionieren.

So rufen Sie den Konfigurationsmodus auf:

1. Vergewissern Sie sich, dass Sie den Administratormodus aufgerufen haben und die Eingabeaufforderung # angezeigt wird.

   Hinweis: Wenn Sie vom Benutzermodus in den Konfigurationsmodus wechseln, verfügen Sie möglicherweise über eingeschränkte Rechte für Konfigurationsänderungen. Siehe **Unterschiedliche CLI-Modi und -Eingabeaufforderungen** *(auf Seite 227).*

2. Geben Sie `config` ein, und drücken Sie die Eingabetaste. Die Eingabeaufforderung "config:#" wird angezeigt und weist darauf hin, dass Sie den Konfigurationsmodus aufgerufen haben.

   ```
   config:# _
   ```

3. Sie können nun einen Konfigurationsbefehl eingeben und die Eingabetaste drücken, um die Einstellungen zu ändern.

Wichtig: Zum Anwenden neuer Konfigurationseinstellungen müssen Sie den Befehl "apply" erteilen, bevor Sie das Terminalemulationsprogramm schließen. Beim Schließen des Programms werden keine Änderungen an der Konfiguration gespeichert. Siehe *Beenden des Konfigurationsmodus* (auf Seite 331).

Befehle zur Gerätekonfiguration

Ein Befehl für die Gerätekonfiguration beginnt mit *emd*. Mit den Befehlen für die Gerätekonfiguration können Sie die Einstellungen ändern, die für das gesamte EMX-Gerät gelten.

Bei den Befehlen ist die Groß-/Kleinschreibung zu beachten.

Ändern des Gerätenamens

Diese Befehlssyntax ändert den Namen des EMX-Geräts.

```
config:#    emd name "<Name>"
```

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die Variable <name> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.

Beispiel

Der folgende Befehl weist dem EMX-Gerät den Namen "my emx888" zu.

```
config:#    emd name "my emx888"
```

Einstellen des Z-Koordinatenformats für Umgebungssensoren

Diese Befehlssyntax aktiviert oder deaktiviert die Verwendung von Gestelleinheiten für die Angabe der Höhe (Z-Koordinate) von Umgebungssensoren.

```
config:#    emd externalSensorsZCoordinateFormat <Option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *rackUnits* oder *freeForm*.

Option	Beschreibung
rackUnits (Gestelleinheiten)	Die Höhe der Z-Koordinate wird in Standard-Rackeinheiten gemessen. Wenn diese Option ausgewählt ist, können Sie einen numerischen Wert für die Rackeinheit eingeben, um die Z-Koordinate von beliebigen Umgebungssensoren zu beschreiben.
freeForm (freie Form)	Zum Angeben der Z-Koordinate können Sie einen beliebigen alphanumerischen String verwenden.

Hinweis: Nach Bestimmung des Formats der Z-Koordinate können Sie einen Wert dafür festlegen. Siehe **Einstellen der Z-Koordinate** *(auf Seite 295).*

Beispiel

Der folgende Befehl bestimmt, dass die Gestelleinheit für die Angabe der Z-Koordinate von Umgebungssensoren verwendet wird.

```
config:#    emd externalSensorsZCoordinateFormat rackUnits
```

Aktivieren oder Deaktivieren des Datenprotokollierung

Diese Befehlssyntax aktiviert oder deaktiviert die Datenprotokollierungsfunktion.

```
config:#    emd dataRetrieval <Option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert die Datenprotokollierungsfunktion.
disable	Deaktiviert die Datenprotokollierungsfunktion.

Weitere Informationen finden Sie unter ***Einrichten der Datenprotokollierung*** (auf Seite 181).

Beispiel

Der folgende Befehl aktiviert die Datenprotokollierungsfunktion.

```
config:#    emd dataRetrieval enable
```

Festlegen der Messungen für die Datenprotokollierung pro Eintrag

Diese Befehlssyntax definiert die Anzahl der Messungen, die pro Protokolleintrag akkumuliert werden.

```
config:#    emd measurementsPerLogEntry <Nummer>
```

Variablen:

- <number> ist ein ganzzahliger Wert zwischen 1 und 600. Der Standardwert lautet 60 Messungen pro Protokolleintrag.

Weitere Informationen finden Sie unter ***Einrichten der Datenprotokollierung*** (auf Seite 181).

Beispiel

Der folgende Befehl legt fest, dass 66 Messungen pro Protokolleintrag für Sensoren akkumuliert werden, d. h. 66 Sekunden.

```
config:#    emd measurementsPerLogEntry 66
```

Befehle für die Netzwerkkonfiguration

Über die CLI kann eine Reihe von Netzwerkeinstellungen geändert werden, wie z. B. die IP-Adresse, die Übertragungsgeschwindigkeit, Duplex-Modus usw.

Festlegen des Netzwerkmodus

Wenn das EMX-Gerät mit der drahtgebundenen und der drahtlosen Netzwerktechnik ausgestattet ist, müssen Sie vor der Konfiguration weiterer Netzwerkparameter festlegen, welche Technik für die Netzwerkverbindung verwendet werden soll.

Diese Befehlssyntax aktiviert den drahtgebundenen oder den drahtlosen Netzwerkmodus.

```
config:#    network mode <mode>
```

Variablen:

- <Modus> ist einer der folgenden Modi: *wired* oder *wireless*.

Modus	Beschreibung
wired	Aktiviert den drahtgebundenen Netzwerkmodus.
wireless	Aktiviert den drahtlosen Netzwerkmodus.

Hinweis: Wenn Sie den drahtlosen Netzwerkmodus aktivieren und die EMX-Einheit keinen drahtlosen USB-LAN-Adapter erkennt oder der angeschlossene drahtlose USB-LAN-Adapter nicht unterstützt wird, wird die Meldung "Supported Wireless device not found" (Kein unterstütztes drahtloses Gerät gefunden) angezeigt.

Beispiel

Der folgende Befehl aktiviert den drahtgebundenen Netzwerkmodus.

```
config:#    network mode wired
```

Konfigurieren der IP-Protokolleinstellungen

Standardmäßig ist nur das IPv4-Protokoll aktiviert. Sie können sowohl das IPv4- als auch das IPv6-Protokoll oder nur das IPv6-Protokoll für das EMX-Gerät aktivieren.

Ein Befehl zur Konfiguration des IP-Protokolls beginnt mit *network ip*.

Aktivieren von IPv4 oder IPv6

Diese Befehlssyntax legt fest, welches IP-Protokoll auf dem EMX-Gerät aktiviert ist.

```
config:#   network ip proto <protocol>
```

Variablen:

- <protocol> ist eine der folgenden Optionen: *v4Only*, *v6Only* oder *both*.

Modus	Beschreibung
v4Only	Aktiviert "IPv4 only" (Nur IPv4) an allen Schnittstellen. Dies ist die Standardeinstellung.
v6Only	Aktiviert "IPv6 only" (Nur IPv6) an allen Schnittstellen.
Both (Beide)	Aktiviert IPv4 und IPv6 an allen Schnittstellen.

Beispiel

Der folgende Befehl legt fest, dass sowohl das IPv4- als auch das IPv6-Protokoll aktiviert ist.

```
config:#   network ip proto both
```

Auswählen der IPv4- oder IPv6-Adressen

Diese Befehlssyntax legt fest, welche IP-Adressen verwendet werden, wenn der DNS-Server IPv4- und IPv6-Adressen zurückgibt. Sie müssen diese Einstellung nur konfigurieren, nachdem das IPv4- und das IPv6-Protokoll auf dem EMX-Gerät aktiviert wurden.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variablen:

- <resolver> ist eine der folgenden Optionen: *preferV4* oder *preferV6.*

Option	Beschreibung
preferV4	Verwenden Sie die vom DNS-Server zurückgegebenen IPv4-Adressen.
preferV6	Verwenden Sie die vom DNS-Server zurückgegebenen IPv6-Adressen.

Beispiel

Der folgende Befehl legt fest, dass nur vom DNS-Server zurückgegebene IPv4-Adressen verwendet werden.

```
config:#   network ip dnsResolverPreference preferV4
```

Einstellen der Parameter für ein drahtloses Netzwerk

Nachdem der Modus für ein drahtloses Netzwerk aktiviert wurde, müssen Sie die Parameter für ein drahtloses Netzwerk konfigurieren, einschließlich SSID (Service Set Identifier), Authentifizierungsmethode, PSK (Pre-Shared Key) und BSSID (Basic Service Set Identifier).

Ein Befehl zur Konfiguration eines drahtlosen Netzwerks beginnt mit *network wireless*.

Hinweis: Wenn der drahtlose Netzwerkmodus nicht als aktueller Netzwerkmodus festgelegt ist, werden die SSID-, PSK- und BSSID-Werte erst angewendet, nachdem der Netzwerkmodus in "wireless" geändert wurde. Zudem wird eine Meldung angezeigt, dass die aktive Netzwerkschnittstelle keine drahtlose Schnittstelle ist.

Bei den Befehlen ist die Groß-/Kleinschreibung zu beachten.

Festlegen der SSID

Diese Befehlssyntax legt den SSID-String fest.

```
config:#   network wireless SSID <ssid>
```

Variablen:

- <ssid> steht für den Namen des drahtlosen Zugangspunkts, der aus Folgendem besteht:

  - Bis zu 32 ASCII-Zeichen

  - Keine Leerzeichen

  - ASCII-Codes 0x20 ~ 0x7E

Beispiel

Der folgende Befehl weist "myssid" als SSID zu.

```
config:#   network wireless SSID myssid
```

Festlegen der Authentifizierungsmethode

Diese Befehlssyntax legt die drahtlose Authentifizierungsmethode auf PSK oder EAP (Extensible Authentication Protocol) fest.

```
config:#   network wireless authMethod <method>
```

Variablen:

- <method> steht für eine der folgenden Authentifizierungsmethoden: *PSK* oder *EAP*.

Methode	Beschreibung
PSK	Die drahtlose Authentifizierungsmethode ist auf PSK festgelegt.
EAP	Die drahtlose Authentifizierungsmethode ist auf EAP festgelegt.

Beispiel

Der folgende Befehl legt die drahtlose Authentifizierungsmethode auf PSK fest.

```
config:#   network wireless authMethod PSK
```

Festlegen von PSK

Wenn die PSK-Authentifizierungsmethode ausgewählt ist, müssen Sie mit der folgenden Befehlssyntax einen PSK-Authentifizierungsschlüssel zuweisen.

```
config:#   network wireless PSK <psk>
```

Variablen:

- <psk> steht für einen String oder einen Authentifizierungsschlüssel, der aus Folgendem besteht:

  - Bis zu 32 ASCII-Zeichen

  - Keine Leerzeichen

  - ASCII-Codes 0x20 ~ 0x7E

Beispiel

Dieser Befehl weist "encryp-key" als PSK zu.

```
config:#   network wireless PSK encryp-key
```

Festlegen der EAP-Parameter

Wenn die drahtlose Authentifizierungsmethode auf EAP festgelegt ist, müssen Sie die EAP-Authentifizierungsparameter konfigurieren, einschließlich äußere Authentifizierung, innere Authentifizierung, EAP-Identität, Kennwort und CA-Zertifikat.

Festlegen der äußeren Authentifizierung

Diese Befehlssyntax legt das Protokoll zur äußeren Authentifizierung für EAP fest.

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

Variablen:

- Der Wert <outer_auth> steht für *PEAP*, weil EMX nur das PEAP (Protected Extensible Authentication Protocol) als äußere Authentifizierung unterstützt.

Beispiel

Der folgende Befehl legt PEAP als das Protokoll zur äußeren Authentifizierung für die EAP-Authentifizierung fest.

```
config:#   network wireless eapOuterAuthentication PEAP
```

Festlegen der inneren Authentifizierung

Diese Befehlssyntax legt das Protokoll zur inneren Authentifizierung für EAP fest.

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

Variablen:

- Der Wert von <inner_auth> ist *MSCHAPv2*, weil EMX nur das Challenge Authentication Protocol Version 2 (MSCHAPv2) von Microsoft als innere Authentifizierung unterstützt.

Beispiel

Der folgende Befehl legt MSCHAPv2 als Protokoll zur inneren Authentifizierung für die EAP-Authentifizierung fest.

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

Festlegen der EAP-Identität

Diese Befehlssyntax legt die EAP-Identität fest.

```
config:#   network wireless eapIdentity <identity>
```

Variablen:

- <identity> ist dabei Ihr Benutzername für die EAP-Authentifizierung.

Beispiel

Der folgende Befehl legt die EAP-Identität auf "eap_user01" fest.

```
config:#   network wireless eapIdentity eap_user01
```

Festlegen des EAP-Kennworts

Diese Befehlssyntax legt das EAP-Kennwort fest.

```
config:#   network wireless eapPassword
```

Variablen:

- <password> ist Ihr Kennwort für die EAP-Authentifizierung.

Beispiel

Der folgende Befehl legt das EAP-Kennwort auf "user01_password" fest.

```
config:#   network wireless eapPassword user01_password
```

Bereitstellen des CA-Zertifikats für EAP

Möglicherweise müssen Sie ein externes CA-Zertifikat für die EAP-Authentifizierung bereitstellen.

So stellen Sie ein CA-Zertifikat bereit:

1. Geben Sie den Befehl für das CA-Zertifikat wie unten gezeigt ein, und drücken Sie die Eingabetaste.

   ```
   config:#   network wireless eapCACertificate
   ```

2. Sie werden aufgefordert, den Inhalt des CA-Zertifikats einzugeben. Gehen Sie zur Eingabe des Inhalts folgendermaßen vor:

   a. Öffnen Sie das CA-Zertifikat mit einem Texteditor.

   b. Kopieren Sie den Inhalt zwischen den Zeilen "--- BEGIN CERTIFICATE ---" und "--- END CERTIFICATE ---" in einem Zertifikat.

   c. Fügen Sie den Inhalt des Zertifikats im Terminal ein.

   d. Drücken Sie die Eingabetaste.

   Tipp: Zum Entfernen eines vorhandenen CA-Zertifikats drücken Sie einfach die Eingabetaste, ohne etwas einzugeben oder einzufügen, wenn Sie zur Eingabe des Zertifikatsinhalts aufgefordert werden.

3. Ist das Zertifikat gültig, wird die Eingabeaufforderung "`config:#`" erneut angezeigt. Falls nicht, weist eine Meldung darauf hin, dass das Zertifikat nicht gültig ist.

Beispiel

Dieser Abschnitt enthält nur ein Beispiel für ein CA-Zertifikat. Der Inhalt Ihres CA-Zertifikats darf nicht mit dem in diesem Beispiel gezeigten Inhalt identisch sein.

So stellen Sie ein CA-Zertifikat bereit:

1. Vergewissern Sie sich, dass Sie sich im Konfigurationsmodus befinden. Siehe ***Aufrufen des Konfigurationsmodus*** (auf Seite 240).
2. Geben Sie den folgenden Befehl ein, und drücken Sie die Eingabetaste.

   ```
   config:#   network wireless eapCACertificate
   ```

3. Sie werden aufgefordert, den Inhalt des CA-Zertifikats einzugeben.
4. Öffnen Sie ein CA-Zertifikat mit einem Texteditor. Der Inhalt des Zertifikats müsste ungefähr wie im Folgenden gezeigt aussehen.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Markieren und kopieren Sie den Inhalt wie unten gezeigt ohne die Anfangszeile "BEGIN CERTIFICATE" und die Endzeile "END CERTIFICATE".

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Fügen Sie den Inhalt in das Terminal ein.
7. Drücken Sie die Eingabetaste.
8. Prüfen Sie, ob die folgende Eingabeaufforderung angezeigt wird. Das bedeutet, dass das bereitgestellte CA-Zertifikat gültig ist.

   ```
   config:#
   ```

Festlegen der BSSID

Diese Befehlssyntax gibt die BSSID an.

```
config:#    network wireless BSSID <bssid>
```

Variablen:

- <bssid> steht für die MAC-Adresse des drahtlosen Zugangspunkts.

Beispiel

Der folgende Befehl gibt an, dass die BSSID 00:14:6C:7E:43:81 lautet.

```
config:#    network wireless BSSID 00:14:6C:7E:43:81
```

Konfigurieren der IPv4-Parameter

Ein Befehl zur IPv4-Konfiguration beginnt mit *network ipv4*.

Bei den Befehlen ist die Groß-/Kleinschreibung zu beachten.

Einstellen des IPv4-Konfigurationsmodus

Diese Befehlssyntax legt den IP-Konfigurationsmodus fest.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variablen:

- <Modus> ist einer der folgenden Modi: *dhcp* oder *static*.

Modus	Beschreibung
dhcp (DHCP)	Der IPv4-Konfigurationsmodus wird auf "DHCP" eingestellt.
static (statisch)	Der IPv4-Konfigurationsmodus wird auf "Statische IP-Adresse" eingestellt.

Beispiel

Der folgende Befehl aktiviert den statischen IP-Konfigurationsmodus.

```
config:#   network ipv4 ipConfigurationMode static
```

Einstellen des bevorzugten Host-Namens

Nachdem Sie "DHCP" als IPv4-Konfigurationsmodus ausgewählt haben, können Sie, falls gewünscht, den bevorzugten Host-Namen angeben. Die Befehlssyntax lautet wie folgt:

```
config:#   network ipv4 preferredHostName <name>
```

Variablen:

- <name> ist ein Host-Name, der:
  - Besteht aus alphanumerischen Zeichen und/oder Bindestrichen
  - Darf nicht mit einem Bindestrich beginnen oder enden
  - Darf nicht mehr als 63 Zeichen enthalten
  - Darf keine Interpunktionszeichen, Leerzeichen und andere Symbole enthalten

Beispiel

Der folgende Befehl stellt den bevorzugten Host-Namen auf "my-host" ein.

```
config:#   network ipv4 preferredHostName my-host
```

Einstellen der IPv4-Adresse

Nach Auswahl des statischen IP-Konfigurationsmodus, können Sie dem EMX-Gerät mit dieser Befehlssyntax eine feste IP-Adresse zuweisen.

```
config:#   network ipv4 ipAddress <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse, die dem EMX-Gerät zugewiesen wird. Der Wert liegt zwischen 0.0.0.0 und 255.255.255.255.

Beispiel

Der folgende Befehl weist dem EMX-Gerät die statische IPv4-Adresse "192.168.84.222" zu.

```
config:#   network ipv4 ipAddress 192.168.84.222
```

Einstellen der IPv4-Subnetzmaske

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax die Subnetzmaske definieren.

```
config:#   network ipv4 subnetMask <netmask>
```

Variablen:

- <netmask> ist die Adresse der Subnetzmaske. Der Wert liegt zwischen 0.0.0.0 und 255.255.255.255.

Beispiel

Der folgende Befehl stellt die Subnetzmaske auf 192.168.84.0 ein.

```
config:#   network ipv4 subnetMask 192.168.84.0
```

Einstellen des IPv4-Gateways

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax das Gateway angeben.

```
config:#   network ipv4 gateway <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des Gateways. Der Wert liegt zwischen 0.0.0.0 und 255.255.255.255.

Beispiel

Der folgende Befehl stellt das IPv4-Gateway auf 255.255.255.0 ein.

```
config:#   network ipv4 gateway 255.255.255.0
```

Einstellen des primären IPv4-DNS-Servers

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax den primären DNS-Server angeben.

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des primären DNS-Servers. Der Wert liegt zwischen 0.0.0.0 und 255.255.255.255.

Beispiel

Der folgende Befehl bestimmt, dass der primäre DNS-Server 192.168.84.30 lautet.

```
config:#   network ipv4 primaryDNSServer 192.168.84.30
```

Einstellen des sekundären IPv4-DNS-Servers

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax den sekundären DNS-Server angeben.

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des sekundären DNS-Servers. Der Wert liegt zwischen 0.0.0.0 und 255.255.255.255.

Hinweis: Die EMX-Einheit unterstützt maximal 3 DNS-Server. Wenn zwei IPv4-DNS-Server und zwei IPv6-DNS-Server zur Verfügung stehen, verwendet die EMX-Einheit nur die primären IPv4- und IPv6-DNS-Server.

Beispiel

Der folgende Befehl bestimmt, dass der sekundäre DNS-Server 192.168.84.33 lautet.

```
config:#   network ipv4 secondaryDNSServer 192.168.84.33
```

Überschreiben des über IPv4-DHCP zugewiesenen DNS-Servers

Nach Angabe des primären/sekundären DNS-Servers können Sie mit diesem Befehl den über DHCP zugewiesenen DNS-Server durch den von Ihnen angegebenen Server ersetzen.

```
config:#   network ipv4 overrideDNS <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Diese Option überschreibt den über DHCP zugewiesenen DNS-Server mit dem von Ihnen zugewiesenen primären/sekundären DNS-Server.
disable	Mit dieser Option wird wieder der über DHCP zugewiesene DNS-Server verwendet.

Beispiel

Der folgende Befehl überschreibt den über DHCP zugewiesenen DNS-Server mit dem von Ihnen angegebenen Server.

```
config:#   network ipv4 overrideDNS enable
```

Konfigurieren der IPv6-Parameter

Ein Befehl zur IPv6-Konfiguration beginnt mit *network ipv6*.

Bei den Befehlen ist die Groß-/Kleinschreibung zu beachten.

Einstellen des IPv6-Konfigurationsmodus

Diese Befehlssyntax legt den IP-Konfigurationsmodus fest.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variablen:

- <Modus> ist einer der folgenden Modi: *automatic* oder *static*.

Modus	Beschreibung
automatic	Der IPv6-Konfigurationsmodus wird auf "automatisch" eingestellt.
static (statisch)	Der IPv6-Konfigurationsmodus wird auf "Statische IP-Adresse" eingestellt.

Beispiel

Der folgende Befehl legt den IP-Konfigurationsmodus auf den Modus für eine statische IP-Adresse fest.

```
config:#   network ipv6 ipConfigurationMode static
```

Einstellen der IPv6-Adresse

Nach Auswahl des statischen IP-Konfigurationsmodus, können Sie dem EMX-Gerät mit dieser Befehlssyntax eine feste IP-Adresse zuweisen.

```
config:#   network ipv6 ipAddress <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse, die dem EMX-Gerät zugewiesen wird. Dieser Wert verwendet das IPv6-Adressformat.

Beispiel

Der folgende Befehl weist dem EMX-Gerät die statische IPv6-Adresse "3210:4179:0:8:0:800:200C:417A" zu.

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

Einstellen des IPv6-Gateways

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax das Gateway angeben.

```
config:#   network ipv6 gateway <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des Gateways. Dieser Wert verwendet das IPv6-Adressformat.

Beispiel

Der folgende Befehl legt das Gateway auf 500:0:330:0:4:9:3:2 fest.

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

Einstellen des primären IPv6-DNS-Servers

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax den primären DNS-Server angeben. Sie ist erforderlich, um ein Überschreiben des automatisch zugewiesenen DNS-Servers zu ermöglichen, bevor Sie die DNS-Server manuell angeben können. Siehe ***Überschreiben des über IPv6-DHCP zugewiesenen DNS-Servers*** (auf Seite 260).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des primären DNS-Servers. Dieser Wert verwendet das IPv6-Adressformat.

Beispiel

Der folgende Befehl legt fest, dass der primäre DNS-Server 2103:288:8201:1::14 ist.

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

Einstellen des sekundären IPv6-DNS-Servers

Nach Wahl des statischen IP-Konfigurationsmodus können Sie mit dieser Befehlssyntax den sekundären DNS-Server angeben. Sie ist erforderlich, um ein Überschreiben des automatisch zugewiesenen DNS-Servers zu ermöglichen, bevor Sie die DNS-Server manuell angeben können. Siehe ***Überschreiben des über IPv6-DHCP zugewiesenen DNS-Servers*** (auf Seite 260).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variablen:

- <ip address> ist die IP-Adresse des sekundären DNS-Servers. Dieser Wert verwendet das IPv6-Adressformat.

Hinweis: Die EMX-Einheit unterstützt maximal 3 DNS-Server. Wenn zwei IPv4-DNS-Server und zwei IPv6-DNS-Server zur Verfügung stehen, verwendet die EMX-Einheit nur die primären IPv4- und IPv6-DNS-Server.

Beispiel

Der folgende Befehl legt fest, dass der sekundäre DNS-Server 2103:288:8201:1::700.

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

Überschreiben des über IPv6-DHCP zugewiesenen DNS-Servers

Nach Angabe des primären/sekundären DNS-Servers können Sie mit diesem Befehl den über DHCP zugewiesenen DNS-Server durch den von Ihnen angegebenen Server ersetzen.

```
config:#   network ipv6 overrideDNS <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Diese Option überschreibt den über DHCP zugewiesenen DNS-Server mit dem von Ihnen zugewiesenen primären/sekundären DNS-Server.
disable	Mit dieser Option wird wieder der über DHCP zugewiesene DNS-Server verwendet.

Beispiel

Der folgende Befehl überschreibt den über DHCP zugewiesenen DNS-Server mit dem von Ihnen angegebenen Server.

```
config:#   network ipv6 overrideDNS enable
```

Festlegen der LAN-Schnittstellenparameter

Ein Befehl zur LAN-Schnittstellenkonfiguration beginnt mit *network interface*.

Bei den Befehlen ist die Groß-/Kleinschreibung zu beachten.

Ändern der Geschwindigkeit der LAN-Schnittstelle

Diese Befehlssyntax bestimmt die Geschwindigkeit der LAN-Schnittstelle.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *auto*, *10Mbps* und *100Mbps*.

Option	Beschreibung
auto	Das System legt die optimale LAN-Geschwindigkeit mithilfe der automatischen Aushandlung fest.
10Mbps	Die LAN-Geschwindigkeit beträgt immer 10 Mbps.
100Mbps	Die LAN-Geschwindigkeit beträgt immer 100 Mbps.

Beispiel

Mit dem folgenden Befehl bestimmt das EMX-Gerät die optimale Geschwindigkeit für die LAN-Schnittstelle per automatischer Aushandlung.

```
config:#   network interface LANInterfaceSpeed auto
```

Ändern des LAN-Duplex-Modus

Diese Befehlssyntax bestimmt den Duplex-Modus der LAN-Schnittstelle.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variablen:

- <Modus> ist einer der folgenden Modi: *auto*, *half* oder *full*.

Option	Beschreibung
auto	Die EMX-Einheit wählt den optimalen Übertragungsmodus mithilfe der automatischen Aushandlung aus.
half	Half duplex (Halbduplex): Daten werden jeweils in eine Richtung übertragen (zu oder von EMX).

Option	Beschreibung
full	Full duplex (Vollduplex): Daten werden gleichzeitig in beide Richtungen übertragen.

Beispiel

Mit dem folgenden Befehl bestimmt das EMX-Gerät den optimalen Übertragungsmodus per automatischer Aushandlung.

```
config:#   network interface LANInterfaceDuplexMode auto
```

Einstellen der Netzwerkdienstparameter

Ein Befehl für Netzwerkdienste beginnt mit *network services*.

Ändern des HTTP-Ports

Diese Befehlssyntax ändert den HTTP-Port.

```
config:#   network services http <n>
```

Variablen:

- <n> ist eine TCP-Portnummer zwischen 1 und 65535. Der Standard-HTTP-Port lautet 80.

Beispiel

Der folgende Befehl stellt den HTTP-Port auf 81 ein.

```
config:#   network services http 81
```

Ändern des HTTPS-Ports

Diese Befehlssyntax ändert den HTTPS-Port.

```
config:#   network services https <n>
```

Variablen:

- <n> ist eine TCP-Portnummer zwischen 1 und 65535. Der Standard-HTTPS-Port lautet 443.

Beispiel

Der folgende Befehl stellt den HTTPS-Port auf 333 ein.

```
config:#   network services https 333
```

Ändern der Telnet-Konfiguration

Sie können den Telnet-Dienst mit den CLI-Befehlen aktivieren oder deaktivieren oder seinen TCP-Port ändern.

Ein Telnet-Befehl beginnt mit *network services telnet*.

Aktivieren oder Deaktivieren von Telnet

Diese Befehlssyntax aktiviert oder deaktiviert den Telnet-Dienst.

```
config:#   network services telnet enabled <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Der Telnet-Dienst wird aktiviert.
false	Der Telnet-Dienst wird deaktiviert.

Beispiel

Der folgende Befehl aktiviert den Telnet-Dienst.

```
config:#   network services telnet enabled true
```

Ändern des Telnet-Ports

Diese Befehlssyntax ändert den Telnet-Port.

```
config:#   network services telnet port <n>
```

Variablen:

- <n> ist dabei eine TCP-Portnummer zwischen 1 und 65535. Der Telnet-Standardport ist 23.

Beispiel

Die folgende Befehlssyntax legt den TCP-Port für Telnet auf 44 fest.

```
config:#   network services telnet port 44
```

Ändern der SSH-Konfiguration

Sie können den SSH-Dienst mit den CLI-Befehlen aktivieren oder deaktivieren oder seinen TCP-Port ändern.

Ein SSH-Befehl beginnt mit *network services ssh*.

Aktivieren oder Deaktivieren von SSH

Diese Befehlssyntax aktiviert oder deaktiviert den SSH-Dienst.

```
config:#   network services ssh enabled <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Der SSH-Dienst wird aktiviert.
false	Der SSH-Dienst wird deaktiviert.

Beispiel

Der folgende Befehl aktiviert den SSH-Dienst.

```
config:#   network services ssh enabled true
```

Ändern des SSH-Ports

Diese Befehlssyntax ändert den SSH-Port.

```
config:#   network services ssh port <n>
```

Variablen:

- <n> ist dabei eine TCP-Portnummer zwischen 1 und 65535. Der SSH-Standardport ist 22.

Beispiel

Die folgende Befehlssyntax legt den TCP-Port für SSH auf 555 fest.

```
config:#   network services ssh port 555
```

Festlegen der SSH-Authentifizierungsmethode

Diese Befehlssyntax legt die SSH-Authentifizierungsmethode fest.

```
config:#   network services ssh authentication <Auth_methode>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *passwordOnly*, *publicKeyOnly* oder *passwordOrPublicKey*.

Option	Beschreibung
passwordOnly	Aktiviert nur die kennwortbasierte Anmeldung.
publicKeyOnly	Aktiviert nur die Anmeldung auf Basis eines öffentlichen Schlüssels.
passwordOrPublicKey	Aktiviert sowohl die Anmeldung auf Kennwortbasis als auch auf Basis des öffentlichen Schlüssels. Dies ist die Standardeinstellung.

Wenn die Authentifizierung mit öffentlichem Schlüssel ausgewählt ist, müssen Sie für jedes Benutzerprofil einen gültigen öffentlichen SSH-Schlüssel eingeben, um sich über die SSH-Verbindung anmelden zu können. Siehe ***Angeben des öffentlichen SSH-Schlüssels*** (auf Seite 314).

Beispiel

Der folgende Befehl hat zur Folge, dass Benutzer ein Kennwort für die SSH-Anmeldung eingeben müssen. Der öffentliche SSH-Schlüssel darf nicht verwendet werden.

```
config:#   network services ssh authentication passwordOnly
```

Festlegen der SNMP-Konfiguration

Mit den CLI-Befehlen können Sie den SNMP v1/v2c- oder v3-Agent aktivieren oder deaktivieren, die Lese- und Schreib-Community-Strings konfigurieren oder die MIB-II-Parameter wie sysContact festlegen.

Ein SNMP-Befehl beginnt mit *network services snmp*.

Aktiveren oder Deaktivieren von SNMP v1/v2c

Diese Befehlssyntax aktiviert oder deaktiviert das SNMP v1/v2c-Protokoll.

```
config:#   network services snmp v1/v2c <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Das SNMP v1/v2c-Protokoll wird aktiviert.
disable	Das SNMP v1/v2c-Protokoll wird deaktiviert.

Beispiel

Der folgende Befehl aktiviert das SNMP v1/v2c-Protokoll.

```
config:#   network services snmp v1/v2c enable
```

Aktivieren oder Deaktivieren von SNMP v3

Diese Befehlssyntax aktiviert oder deaktiviert das SNMP v3-Protokoll.

```
config:#   network services snmp v3 <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Das SNMP v3-Protokoll wird aktiviert.
disable	Das SNMP v3-Protokoll wird deaktiviert.

Beispiel

Der folgende Befehl aktiviert das SNMP v3-Protokoll.

```
config:#   network services snmp v3 enable
```

Festlegen der Lese-Community für SNMP

Diese Befehlssyntax legt den Lese-Community-String für SNMP fest.

```
config:#   network services snmp readCommunity <string>
```

Variablen:

- <string> ist ein String, der 4 bis 64 druckbare ASCII-Zeichen enthält.
- In dem String DÜRFEN KEINE Leerzeichen enthalten sein.

Beispiel

Diese Befehlssyntax legt den Lese-Community-String für SNMP auf "public" fest.

```
config:#   network services snmp readCommunity public
```

Festlegen der Schreib-Community für SNMP

Diese Befehlssyntax legt den Schreib-Community-String für SNMP fest.

```
config:#   network services snmp writeCommunity <string>
```

Variablen:

- <string> ist ein String, der 4 bis 64 druckbare ASCII-Zeichen enthält.
- In dem String DÜRFEN KEINE Leerzeichen enthalten sein.

Beispiel

Der folgende Befehl legt den Schreib-Community-String für SNMP auf "private" fest.

```
config:#   network services snmp writeCommunity private
```

Festlegen des sysContact-Werts

Diese Befehlssyntax legt den sysContact-MIB-II-Wert für SNMP fest.

```
config:#   network services snmp sysContact <value>
```

Variablen:

- <value> ist ein String, der 0 bis 255 alphanumerische Zeichen enthält.

Beispiel

Der folgende Befehl legt den MIB-II-sysContact-Wert für SNMP auf "John_Krause" fest.

```
config:#   network services snmp sysContact John_Krause
```

Festlegen des sysName-Werts

Diese Befehlssyntax legt den sysName-MIB-II-Wert für SNMP fest.

```
config:#   network services snmp sysName <value>
```

Variablen:

- <value> ist ein String, der 0 bis 255 alphanumerische Zeichen enthält.

Beispiel

Der folgende Befehl legt den MIB-II-sysName-Wert für SNMP auf "Win7_system" fest.

```
config:#   network services snmp sysName Win7_system
```

Festlegen des sysLocation-Werts

Diese Befehlssyntax legt den sysLocation-MIB-II-Wert für SNMP fest.

```
config:#   network services snmp sysLocation <value>
```

Variablen:

- <value> ist ein String, der 0 bis 255 alphanumerische Zeichen enthält.

Beispiel

Der folgende Befehl legt den MIB-II-sysLocation-Wert für SNMP auf "New_TAIPEI" fest.

```
config:#   network services snmp sysLocation New_TAIPEI
```

Befehle für die Sicherheitskonfiguration

Ein Befehl für die Sicherheitskonfiguration beginnt mit *security*.

Firewall-Steuerung

Sie können Steuerungsfunktionen für die Firewall über die CLI verwalten. Mit der Firewall-Steuerung lassen sich Regeln einrichten, die den Zugriff auf das EMX-Gerät von bestimmten IP-Adressen oder einem IP-Adressbereich zulassen oder verweigern.

- Ein Befehl zur IPv4-Firewall-Konfiguration beginnt mit *security ipAccessControl ipv4*.
- Ein Befehl zur IPv6-Firewall-Konfiguration beginnt mit *security ipAccessControl ipv6*.

Ändern der Parameter für die Firewall-Steuerung

Zum Ändern der Parameter für die Firewall-Steuerung stehen verschiedene Befehle zur Verfügung.

- **IPv4-Befehle**

Verwenden Sie die folgende Befehlssyntax, um die Funktion zur IPv4-Firewall-Steuerung zu aktivieren oder zu deaktivieren:

```
config:#    security ipAccessControl ipv4 enabled <option>
```

Verwenden Sie die folgende Befehlssyntax, um die Standardrichtlinie für die IPv4-Firewall-Steuerung festzulegen:

```
config:#    security ipAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6-Befehle**

Verwenden Sie die folgende Befehlssyntax, um die Funktion zur IPv6-Firewall-Steuerung zu aktivieren oder zu deaktivieren:

```
config:#    security ipAccessControl ipv6 enabled <option>
```

Verwenden Sie die folgende Befehlssyntax, um die Standardrichtlinie für die IPv6-Firewall-Steuerung festzulegen:

```
config:#    security ipAccessControl ipv6 defaultPolicy <policy>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Aktiviert die Funktion für die IP-Zugriffssteuerung.
false	Deaktiviert die Funktion für die IP-Zugriffssteuerung.

- <policy> ist eine der folgenden Optionen: *accept* (zulassen), *drop* (trennen) oder *reject* (ablehnen).

Option	Beschreibung
accept	Lässt Verkehr von allen IP-Adressen zu.

Option	Beschreibung
drop	Verwirft den Verkehr von allen IP-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
reject	Verwirft den Verkehr von allen IP-Adressen und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.

Tipp: Sie können beide Befehle kombinieren, um alle Parameter für die Firewall-Steuerung gleichzeitig zu ändern. Siehe **Multi-Befehlssyntax** *(auf Seite 330).*

Beispiel

Der folgende Befehl richtet zwei Parameter der Funktion für die IPv4-Zugriffssteuerung ein.

```
config:#   security ipAccessControl ipv4 enabled true defaultPolicy accept
```

Ergebnisse:

- Die Funktion für die IPv4-Zugriffssteuerung wird aktiviert.
- Die Standardrichtlinie ist auf "accept" festgelegt.

Verwalten von Firewall-Regeln

Sie können Firewall-Regeln mit den CLI-Befehlen hinzufügen, löschen oder ändern.

- Ein Befehl für die IPv4-Firewall-Steuerungsregel beginnt mit *security ipAccessControl ipv4 rule*.
- Ein Befehl für die IPv6-Firewall-Steuerungsregel beginnt mit *security ipAccessControl ipv6 rule*.

Hinzufügen einer Firewall-Regel

Die Befehlssyntax zum Hinzufügen einer Regel variiert abhängig davon, wo Sie eine neue Firewall-Regel in der Liste hinzufügen möchten.

- **IPv4-Befehle**

▸ **Verwenden Sie die folgende Befehlssyntax, um eine neue Regel am Ende der IPv4-Regelliste hinzuzufügen:**

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy>
```

Verwenden Sie die folgende Befehlssyntax, um eine neue IPv4-Regel oberhalb oder unterhalb einer bestimmten Regel einzufügen:

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy> <insert>
            <rule_number>
```

-- ODER --

```
config:#    security ipAccessControl ipv4 rule add <insert> <rule_number> <ip_mask>
            <policy>
```

- **IPv6-Befehle**

Verwenden Sie die folgende Befehlssyntax, um eine neue Regel am Ende der IPv6-Regelliste hinzuzufügen:

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy>
```

Verwenden Sie die folgende Befehlssyntax, um eine neue IPv6-Regel oberhalb oder unterhalb einer bestimmten Regel einzufügen:

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy> <insert> <rule_number>
```

-- ODER --

```
config:#    security ipAccessControl ipv6 rule add <insert> <rule_number> <ip_mask> <policy>
```

Variablen:

- <ip_mask> ist die Kombination der Werte für IP-Adresse und Subnetzmaske, die durch einen Schrägstrich getrennt sind. Eine IPv4-Kombination sieht z. B. folgendermaßen aus: *192.168.94.222/24*.
- <policy> ist eine der folgenden Optionen: *accept* (zulassen), *drop* (trennen) oder *reject* (ablehnen).

Richtlinie	Beschreibung
accept	Lässt Verkehr von den angegebenen IP-Adressen zu.

Richtlinie	Beschreibung
drop	Verwirft den Verkehr von den angegebenen IP-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
reject	Verwirft den Verkehr von den angegebenen IP-Adressen und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.

- <insert> ist eine der folgenden Optionen: *insertAbove* (davor einfügen) oder *insertBelow* (danach einfügen).

Option	Beschreibung
insertAbove	Fügt die neue Regel vor der angegebenen Regelnummer ein. Gehen Sie anschließend wie folgt vor: Nummer der neuen Regel = die angegebene Regelnummer
insertBelow	Fügt die neue Regel nach der angegebenen Regelnummer ein. Gehen Sie anschließend wie folgt vor: Nummer der neuen Regel = die angegebene Regelnummer + 1

- <rule_number> ist die Nummer der bestehenden Regel, vor oder nach der Sie die neue Regel einfügen möchten.

Beispiel

Der folgende Befehl fügt eine neue Regel für die IPv4-Zugriffssteuerung hinzu und gibt ihre Position in der Liste an.

```
config:#   security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
           insertAbove 5
```

Ergebnisse:

- Es wird eine neue Regel zur IPv4-Firewall-Steuerung hinzugefügt, die zulässt, dass alle Pakete der IPv4-Adresse 192.168.84.123 akzeptiert werden.
- Die hinzugefügte Regel wird über der 5. Regel eingefügt. Das bedeutet, dass die neue Regel zur 5. Regel und die ursprünglich 5. Regel zur 6. Regel wird.

Ändern einer Firewall-Regel

Die Befehlssyntax variiert abhängig davon, was in einer vorhandenen Regel geändert werden soll.

- **IPv4-Befehle**

Befehlssyntax zum Ändern der IP-Adresse und/oder Subnetzmaske einer IPv4-Regel:

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>
```

Befehlssyntax zum Ändern der Richtlinie einer IPv4-Regel:

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> policy <policy>
```

Befehlssyntax zum Ändern des gesamten Inhalts einer vorhandenen IPv4-Regel:

```
config:#  security ipAccessControl ipv4 rule modify <rule_number> ipMask <ip_mask>
          policy <policy>
```

- **IPv6-Befehle**

Befehlssyntax zum Ändern der IP-Adresse und/oder Subnetzmaske einer IPv6-Regel:

```
config:#  security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
```

Befehlssyntax zum Ändern der Richtlinie einer IPv6-Regel:

```
config:#  security ipAccessControl ipv6 rule modify <rule_number> policy <policy>
```

Befehlssyntax zum Ändern des gesamten Inhalts einer vorhandenen IPv6-Regel:

```
config:#    security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
            policy <policy>
```

Variablen:

- <rule_number> ist die Nummer der bestehenden Regel, die Sie ändern möchten.
- <ip_mask> ist die Kombination der Werte für IP-Adresse und Subnetzmaske, die durch einen Schrägstrich getrennt sind. Eine IPv4-Kombination sieht z. B. folgendermaßen aus: *192.168.94.222/24*.
- <policy> ist eine der folgenden Optionen: *accept* (zulassen), *drop* (trennen) oder *reject* (ablehnen).

Option	Beschreibung
accept	Lässt Verkehr von den angegebenen IP-Adressen zu.
drop	Verwirft den Verkehr von den angegebenen IP-Adressen, ohne den Quell-Host über den Fehler zu benachrichtigen.
reject	Verwirft den Verkehr von den angegebenen IP-Adressen und eine IMCP-Meldung wird an den Quell-Host gesendet, um ihn über den Fehler zu benachrichtigen.

Beispiel

Der folgende Befehl ändert den gesamten Inhalt der 5. IPv4-Regel.

```
config:#    security ipAccessControl ipv4 rule modify 5 ipMask 192.168.84.123/24
            policy accept
```

Ergebnisse:

- Die IPv4-Adresse wird in 192.168.84.123 und die Subnetzmaske in 255.255.255.0 geändert.
- Die Richtlinie lautet nun "accept".

Löschen einer Firewall-Regel

Die folgenden Befehle entfernen eine bestimmte IPv4- oder IPv6-Regel aus der Liste.

- **IPv4-Befehle**

```
config:#    security ipAccessControl ipv4 rule delete <rule_number>
```

- **IPv6-Befehle**

```
config:#    security ipAccessControl ipv6 rule delete <rule_number>
```

Variablen:

- <rule_number> ist die Nummer der bestehenden Regel, die Sie entfernen möchten.

Beispiel

Der folgende Befehl entfernt die 5. Regel aus der IPv6-Zugriffssteuerungsliste.

```
config:#    security ipAccessControl ipv6 rule delete 5
```

HTTPS-Zugriff

Dieser Befehl legt fest, ob der HTTPS-Zugriff auf die EMX-Webschnittstelle erzwungen wird. Ist dies der Fall, werden alle HTTP-Zugriffsversuche automatisch auf HTTPS umgeleitet.

```
config:#    security enforceHttpsForWebAccess <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert den HTTPS-Zugriff auf die Webschnittstelle.
disable	Deaktiviert den HTTPS-Zugriff auf die Webschnittstelle.

Beispiel

Der folgende Befehl deaktiviert die HTTPS-Zugriffsfunktion.

```
config:#    security enforceHttpsForWebAccess disable
```

Anmeldebeschränkung

Die Funktion zur Anmeldebeschränkung steuert anmeldebezogene Beschränkungen, wie die Kennworterneuerung, die gleichzeitige Anmeldung mit einem einzigen Benutzernamen sowie die zulässige Inaktivitätszeit, bevor eine Abmeldung erzwungen wird.

Ein Befehl zur Anmeldebeschränkung beginnt mit *security loginLimits*.

Sie können mehrere Befehle kombinieren, um die Parameter für die Anmeldebeschränkung gleichzeitig zu ändern. Siehe ***Multi-Befehlssyntax*** (auf Seite 330).

Beschränkung auf Einzelanmeldung

Diese Befehlssyntax aktiviert oder deaktiviert die Einzelanmeldungsfunktion, die steuert, ob gleichzeitig mehrere Anmeldungen mit demselben Anmeldenamen erlaubt sind.

```
config:#   security loginLimits singleLogin <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert die Einzelanmeldungsfunktion.
disable	Deaktiviert die Einzelanmeldungsfunktion.

Beispiel

Der folgende Befehl deaktiviert die Einzelanmeldungsfunktion, sodass sich mehrere Benutzer mit demselben Benutzernamen gleichzeitig anmelden können.

```
config:#   security loginLimits singleLogin disable
```

Kennworterneuerung

Diese Befehlssyntax aktiviert oder deaktiviert die Funktion zur Kennworterneuerung, die steuert, ob das Kennwort regelmäßig geändert werden soll:

```
config:#   security loginLimits passwordAging <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert die Funktion zur Kennworterneuerung.
disable	Deaktiviert die Funktion zur Kennworterneuerung.

Beispiel

Der folgende Befehl aktiviert die Funktion zur Kennworterneuerung.

```
config:#   security loginLimits passwordAging enable
```

Intervall der Kennworterneuerung

Diese Befehlssyntax legt fest, wie oft das Kennwort geändert werden muss.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variablen:

- <value> ist ein numerischer Wert in Tagen, der für das Intervall zur Kennworterneuerung festgelegt wurde. Das Intervall lässt sich auf einen Wert von 7 bis 365 Tagen einstellen.

Beispiel

Der folgende Befehl legt das Intervall für die Kennworterneuerung auf 90 Tage fest.

```
config:#   security loginLimits passwordAgingInterval 90
```

Zeitlimit für Inaktivität

Diese Befehlssyntax legt fest, wie lange ein Benutzer inaktiv sein kann, bevor dieser Benutzer gezwungen wird, sich von der EMX-Webschnittstelle abzumelden.

```
config:#   security loginLimits idleTimeout <value>
```

Variablen:

- <value> ist ein numerischer Wert in Minuten, der für das Inaktivitätszeitlimit festgelegt wurde. Das Zeitlimit lässt sich auf einen Wert von 1 bis 1440 Minuten (24 Stunden) einstellen.

Beispiel

Der folgende Befehl legt das Inaktivitätszeitlimit auf 10 Minuten fest.

```
config:#   security loginLimits idleTimeout 10
```

Benutzersperrung

Es stehen verschiedene Befehle zur Verfügung, mit denen sich verschiedene Parameter für die Benutzersperrung ändern lassen. Diese Befehle beginnen mit `security userBlocking`.

Verwenden Sie die folgende Befehlssyntax, um die maximale Anzahl fehlgeschlagener Anmeldungen festzulegen, bevor ein Benutzer gesperrt wird:

```
config:#    security userBlocking maximumNumberOfFailedLogins <value1>
```

- **Verwenden Sie die folgende Befehlssyntax, um festzulegen, wie lange die Anmeldung eines Benutzers gesperrt wird:**

  ```
  config:#    security userBlocking blockTime <value2>
  ```

Variablen:

- <value1> ist ein ganzzahliger Wert zwischen 3 und 10 oder *unlimited*, der für die maximale Anzahl an fehlgeschlagenen Anmeldungen kein Limit festlegt und die Funktion zur Benutzersperrung somit deaktiviert.
- <value2> ist ein numerischer Wert in Minuten.

Tipp: Sie können mehrere Befehle kombinieren, um die Parameter für die Benutzersperrung gleichzeitig zu ändern. Siehe **Multi-Befehlssyntax** *(auf Seite 330).*

Beispiel

Der folgende Befehl richtet zwei Parameter für die Benutzersperrung ein.

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Ergebnisse:

- Die maximale Anzahl an fehlgeschlagenen Anmeldungen wird auf 5 festgelegt.
- Der Benutzer wird 30 Minuten gesperrt.

Sichere Kennwörter

Die Befehle für sichere Kennwörter legen fest, ob ein sicheres Kennwort für die Anmeldung erforderlich ist und was ein sicheres Kennwort mindestens enthalten muss.

Ein Befehl für sichere Kennwörter beginnt mit `security strongPasswords`.

Sie können mehrere Befehle für sichere Kennwörter kombinieren, um verschiedene Parameter gleichzeitig zu ändern. Siehe ***Multi-Befehlssyntax*** (auf Seite 330).

Aktivieren oder Deaktivieren sicherer Kennwörter

Diese Befehlssyntax aktiviert oder deaktiviert die Funktion für sichere Kennwörter.

```
config:#   security strongPasswords enabled <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Aktiviert die Funktion für sichere Kennwörter.
false	Deaktiviert die Funktion für sichere Kennwörter.

Beispiel

Diese Befehlssyntax aktiviert die Funktion für sichere Kennwörter.

```
config:#   security strongPasswords enabled true
```

Mindestlänge eines Kennworts

Diese Befehlssyntax legt die Mindestlänge des Kennworts fest.

```
config:#   security strongPasswords minimumLength <value>
```

Variablen:

- <value> ist ein ganzzahliger Wert zwischen 8 und 32.

Beispiel

Diese Befehlssyntax legt fest, dass ein Kennwort mindestens 8 Zeichen enthalten muss.

```
config:#    security strongPasswords minimumLength 8
```

Maximale Kennwortlänge

Diese Befehlssyntax legt die maximale Länge des Kennworts fest.

```
config:#    security strongPasswords maximumLength <value>
```

Variablen:

- <value> ist ein ganzzahliger Wert zwischen 16 und 64.

Beispiel

Diese Befehlssyntax legt fest, dass ein Kennwort NICHT mehr als 20 Zeichen enthalten darf.

```
config:#    security strongPasswords maximumLength 20
```

Erforderliche Angabe eines Kleinbuchstabens

Diese Befehlssyntax legt fest, ob ein sicheres Kennwort mindestens einen Kleinbuchstaben enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Mindestens ein Kleinbuchstabe ist erforderlich.
disable	Es ist kein Kleinbuchstabe erforderlich.

Beispiel

Diese Befehlssyntax legt fest, dass ein Kennwort mindestens einen Kleinbuchstaben enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

Erforderliche Angabe eines Großbuchstabens

Diese Befehlssyntax legt fest, ob ein sicheres Kennwort mindestens einen Großbuchstaben enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Mindestens ein Großbuchstabe ist erforderlich.
disable	Es ist kein Großbuchstabe erforderlich.

Beispiel

Dieser Befehl legt fest, dass ein Kennwort mindestens einen Großbuchstaben enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

Erforderliche Angabe einer Ziffer

Diese Befehlssyntax legt fest, ob ein sicheres Kennwort mindestens eine Ziffer enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Mindestens eine Ziffer ist erforderlich.
disable	Es ist keine Ziffer erforderlich.

Beispiel

Der folgende Befehl legt fest, dass ein Kennwort mindestens eine Ziffer enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

Erforderliche Angabe eines Sonderzeichens

Diese Befehlssyntax legt fest, ob ein sicheres Kennwort mindestens ein Sonderzeichen enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Mindestens ein Sonderzeichen ist erforderlich.
disable	Es ist kein Sonderzeichen erforderlich.

Beispiel

Der folgende Befehl legt fest, dass ein Kennwort mindestens ein Sonderzeichen enthalten muss.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

Maximaler Kennwortverlauf

Diese Befehlssyntax legt die Anzahl an vorherigen Kennwörtern fest, die bei einer Kennwortänderung NICHT wiederverwendet werden dürfen.

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

Variablen:

- <value> ist ein ganzzahliger Wert zwischen 1 und 12.

Beispiel

Der folgende Befehl legt fest, dass die vorherigen 7 Kennwörter bei einer Kennwortänderung NICHT wiederverwendet werden dürfen.

```
config:#    security strongPasswords passwordHistoryDepth 7
```

Rollenbasierte Zugriffssteuerung

Neben der Firewall-Zugriffssteuerung auf Basis von IP-Adressen können Sie weitere Regeln für die Zugriffssteuerung konfigurieren, die sowohl auf IP-Adressen als auch auf Rollen (Benutzerfunktionen) basieren.

- Ein Befehl für die rollenbasierte IPv4-Zugriffssteuerung beginnt mit *security roleBasedAccessControl ipv4*.
- Ein Befehl für die rollenbasierte IPv6-Zugriffssteuerung beginnt mit *security roleBasedAccessControl ipv6*.

Ändern von Parametern für die rollenbasierte Zugriffssteuerung

Zum Ändern der Parameter für die rollenbasierte Zugriffssteuerung stehen verschiedene Befehle zur Verfügung.

- **IPv4-Befehle**

Verwenden Sie die folgende Befehlssyntax, um die Funktion zur rollenbasierten IPv4-Zugriffssteuerung zu aktivieren oder zu deaktivieren:

```
config:#    security roleBasedAccessControl ipv4 enabled <option>
```

Verwenden Sie die folgende Befehlssyntax, um die Richtlinie für die rollenbasierte IPv4-Zugriffssteuerung festzulegen:

```
config:#    security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6-Befehle**

Verwenden Sie die folgende Befehlssyntax, um die Funktion zur rollenbasierten IPv6-Zugriffssteuerung zu aktivieren oder zu deaktivieren:

```
config:#    security roleBasedAccessControl ipv6 enabled <option>
```

Verwenden Sie die folgende Befehlssyntax, um die Richtlinie für die rollenbasierte IPv6-Zugriffssteuerung festzulegen:

```
config:#    security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Aktiviert die Funktion für die rollenbasierte Zugriffssteuerung.
false	Deaktiviert die Funktion für die rollenbasierte Zugriffssteuerung.

- <policy> ist eine der folgenden Optionen: *allow* oder *deny*.

Richtlinie	Beschreibung
allow	Lässt Verkehr von allen IP-Adressen zu, unabhängig von der Benutzerfunktion.
deny	Lehnt den Verkehr von allen IP-Adressen ab, unabhängig von der Benutzerfunktion.

Tipp: Sie können beide Befehle kombinieren, um alle Parameter für die rollenbasierte Zugriffssteuerung gleichzeitig zu ändern. Siehe **Multi-Befehlssyntax** *(auf Seite 330).*

Beispiel

Der folgende Befehl legt zwei Parameter der Funktion für die rollenbasierte IPv4-Zugriffssteuerung fest.

```
config:#    security roleBasedAccessControl ipv4 enabled true defaultPolicy allow
```

Ergebnisse:

- Die Funktion für die rollenbasierte IPv4-Zugriffssteuerung wird aktiviert.
- Die Standardrichtlinie ist auf "allow" festgelegt.

Verwalten von Regeln für die rollenbasierte Zugriffssteuerung

Sie können Regeln für die rollenbasierte Zugriffssteuerung hinzufügen, löschen oder ändern.

- Ein Befehl für die rollenbasierte IPv4-Zugriffssteuerung zum Verwalten von Regeln beginnt mit *security roleBasedAccessControl ipv4 rule*.
- Ein Befehl für die rollenbasierte IPv6-Zugriffssteuerung zum Verwalten von Regeln beginnt mit *security roleBasedAccessControl ipv6 rule*.

Hinzufügen einer Regel für die rollenbasierte Zugriffssteuerung

Die Befehlssyntax zum Hinzufügen einer Regel variiert abhängig davon, wo Sie eine neue Regel in der Liste hinzufügen möchten.

- **IPv4-Befehle**

▶ **Verwenden Sie die folgende Befehlssyntax, um eine neue Regel am Ende der IPv4-Regelliste hinzuzufügen:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **Verwenden Sie die folgende Befehlssyntax, um eine neue IPv4-Regel oberhalb oder unterhalb einer bestimmten Regel einzufügen:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
          <insert> <rule_number>
```

- **IPv6-Befehle**

▶ **Verwenden Sie die folgende Befehlssyntax, um eine neue Regel am Ende der IPv6-Regelliste hinzuzufügen:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **Verwenden Sie die folgende Befehlssyntax, um eine neue IPv6-Regel oberhalb oder unterhalb einer bestimmten Regel einzufügen:**

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
           <insert> <rule_number>
```

Variablen:

- <start_ip> ist die IP-Startadresse.
- <end_ip> ist die IP-Endadresse.
- <role> ist die Benutzerfunktion, für die Sie eine Zugriffssteuerungsregel erstellen möchten.
- <policy> ist eine der folgenden Optionen: *allow* oder *deny*.

Richtlinie	Beschreibung
allow	Lässt den Verkehr von dem angegebenen IP-Adressbereich zu, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist
deny	Lehnt den Verkehr von dem angegebenen IP-Adressbereich ab, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist

- <insert> ist eine der folgenden Optionen: *insertAbove* (davor einfügen) oder *insertBelow* (danach einfügen).

Option	Beschreibung
insertAbove	Fügt die neue Regel vor der angegebenen Regelnummer ein. Gehen Sie anschließend wie folgt vor: Nummer der neuen Regel = die angegebene Regelnummer
insertBelow	Fügt die neue Regel nach der angegebenen Regelnummer ein. Gehen Sie anschließend wie folgt vor: Nummer der neuen Regel = die angegebene Regelnummer + 1

- <rule_number> ist die Nummer der bestehenden Regel, vor oder nach der Sie die neue Regel einfügen möchten.

Beispiel

Der folgende Befehl erstellt eine neue Regel für die rollenbasierte IPv4-Zugriffssteuerung und gibt ihre Position in der Liste an.

```
config:#    security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin
            deny insertAbove 3
```

Ergebnisse:

- Eine neue Regel für die rollenbasierte IPv4-Zugriffssteuerung wird hinzugefügt, die alle Pakete der IPv4-Adressen zwischen 192.168.78.50 und 192.168.90.100 ablehnt, wenn der Benutzer zur Benutzerfunktion "admin" gehört.
- Die hinzugefügte IPv4-Regel wird über der 3. Regel eingefügt. Das bedeutet, dass die neue Regel zur 3. Regel und die ursprünglich 3. Regel zur 4. Regel wird.

Ändern einer Regel für die rollenbasierte Zugriffssteuerung

Die Befehlssyntax variiert abhängig davon, was in einer vorhandenen Regel geändert werden soll.

- **IPv4-Befehle**

Verwenden Sie die folgende Befehlssyntax, um den IPv4-Adressbereich einer Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

Verwenden Sie die folgende Befehlssyntax, um die Benutzerfunktion einer IPv4-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

Verwenden Sie die folgende Befehlssyntax, um die Richtlinie einer IPv4-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> policy
            <policy>
```

Verwenden Sie diese Befehlssyntax, um den gesamten Inhalt einer vorhandenen IPv4-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- **IPv6-Befehle**

Verwenden Sie die folgende Befehlssyntax, um den IPv6-Adressbereich einer Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

Verwenden Sie die folgende Befehlssyntax, um die Benutzerfunktion einer IPv6-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

Verwenden Sie die folgende Befehlssyntax, um die Richtlinie einer IPv6-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

Verwenden Sie diese Befehlssyntax, um den gesamten Inhalt einer vorhandenen IPv6-Regel zu ändern:

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variablen:

- <rule_number> ist die Nummer der bestehenden Regel, die Sie ändern möchten.
- <start_ip> ist die IP-Startadresse.
- <end_ip> ist die IP-Endadresse.
- <role> ist dabei eine der bestehenden Benutzerfunktionen.
- <policy> ist eine der folgenden Optionen: *allow* oder *deny*.

Richtlinie	Beschreibung
allow	Lässt den Verkehr von dem angegebenen IP-Adressbereich zu, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist

Richtlinie	Beschreibung
deny	Lehnt den Verkehr von dem angegebenen IP-Adressbereich ab, wenn der Benutzer ein Mitglied der angegebenen Benutzerfunktion ist

Beispiel

Der folgende Befehl ändert den gesamten Inhalt der 8. IPv4-Regel.

```
config:#   security roleBasedAccessControl ipv4 rule modify 8
           startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
           policy allow
```

Ergebnisse:

- Die IPv4-Startadresse wird in 192.168.8.8 und die IPv4-Endadresse in 192.168.90.90 geändert.
- Die Benutzerfunktion wird in "operator" geändert.
- Die Richtlinie lautet nun "allow".

Löschen einer Regel für die rollenbasierte Zugriffssteuerung

Dieser Befehl entfernt eine bestimmte Regel aus der Liste.

- **IPv4-Befehle**

```
config:#   security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- **IPv6-Befehle**

```
config:#   security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variablen:

- <rule_number> ist die Nummer der bestehenden Regel, die Sie entfernen möchten.

Beispiel

Der folgende Befehl entfernt die 7. IPv6-Regel.

```
config:#   security roleBasedAccessControl ipv6 rule delete 7
```

Befehle für die Umgebungssensorkonfiguration

Ein Befehl für die Umgebungssensorkonfiguration beginnt mit *externalsensor*. Sie können die Namens- und Standortparameter eines einzelnen Umgebungssensors konfigurieren.

Ändern des Sensornamens

Diese Befehlssyntax benennt einen Umgebungssensor.

```
config:#   externalsensor <n> name "<name>"
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die Variable <name> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.

Beispiel

Der folgende Befehl weist dem Umgebungssensor mit ID Nummer 4 den Namen "Cabinet humidity" zu.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Angeben des Sensortyps

Der Kontaktschlusssensor (DPX-CC2-TR) von Raritan unterstützt den Anschluss verschiedener externer Detektoren/Schalter; für einen ordnungsgemäßen Betrieb müssen Sie den Typ des angeschlossenen Detektors/Schalters angeben. Verwenden Sie die folgende Befehlssyntax, wenn Sie den Sensortyp angeben müssen.

```
config:#   externalsensor <n> sensorSubType <type>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <type> bezeichnet einen der folgenden Sensortypen: *contact*, *smokeDetection*, *waterDetection* oder *vibration*.

Typ	Beschreibung
contact	Der angeschlossene Detektor/Schalter erkennt den Türschlossstatus oder den Status "Tür geschlossen/offen".
smokeDetection	Der angeschlossene Detektor/Schalter erkennt, ob Rauch vorhanden ist.
waterDetection	Der angeschlossene Detektor/Schalter erkennt, ob Wasser vorhanden ist.
vibration	Der angeschlossene Detektor/Schalter erkennt Erschütterungen.

Beispiel

Der folgende String gibt an, dass ein Rauchmelder an den Raritan-Kontaktschlusssensor (DPX-CC2-TR) angeschlossen ist, dessen ID-Nummer in der EMX-Webschnittstelle 2 lautet.

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

Einstellen der X-Koordinate

Diese Befehlssyntax gibt die X-Koordinate eines Umgebungssensors an.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Koordinate> ist ein String, der maximal 24 druckbare ASCII-Zeichen enthält und in Anführungszeichen stehen muss.

Beispiel

Der folgende Befehl setzt den Wert "The 2nd cabinet" für die X-Koordinate des Umgebungssensors mit ID Nummer 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Einstellen der Y-Koordinate

Diese Befehlssyntax gibt die Y-Koordinate eines Umgebungssensors an.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Koordinate> ist ein String, der maximal 24 druckbare ASCII-Zeichen enthält und in Anführungszeichen stehen muss.

Beispiel

Der folgende Befehl setzt den Wert "The 4th row" für die Y-Koordinate des Umgebungssensors mit ID Nummer 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Einstellen der Z-Koordinate

Diese Befehlssyntax gibt die Z-Koordinate eines Umgebungssensors an.

config:# externalsensor <n> zlabel "<coordinate>"

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- Abhängig von der von Ihnen festgelegten Z-Koordinate gibt es zwei Arten von Werten für die Variable <coordinate>:

Typ	Beschreibung
Free form (Freie Form)	<Koordinate> ist ein String, der maximal 24 druckbare ASCII-Zeichen enthält und in Anführungszeichen stehen muss.
Rack units (Rackeinheiten)	<coordinate> ist ein ganzzahliger Wert in Rackeinheiten.

Hinweis: Sie können mithilfe der Rackeinheiten die Z-Koordinate angeben. Siehe **Einstellen des Z-Koordinatenformats für Umgebungssensoren** *(auf Seite 242).*

Beispiel

Der folgende Befehl setzt den Wert "The 5th rack" für die Z-Koordinate des Umgebungssensors mit der ID-Nummer 4, nachdem das Format der Z-Koordinate auf *freeForm* (Freie Form) eingestellt wurde.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Ändern der Sensorbeschreibung

Diese Befehlssyntax stellt eine Beschreibung für einen bestimmten Umgebungssensor bereit.

```
config:#   externalsensor <n> description "<description>"
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <description> ist ein String, der maximal 64 druckbare ASCII-Zeichen enthält und in Anführungszeichen stehen muss.

Beispiel

Der folgende Befehl weist dem Umgebungssensor mit der ID-Nummer 4 die Beschreibung "humidity detection" zu.

```
config:#   externalsensor 4 description "humidity detection"
```

Befehle für die Konfiguration von Umgebungssensorschwellenwerten

Ein Befehl für die Sensorschwellenwert-Konfiguration für Umgebungssensoren beginnt mit *sensor externalsensor*.

Einstellen des oberen kritischen Schwellenwerts für den Sensor

Diese Befehlssyntax konfiguriert den oberen kritischen Schwellenwert eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <Option> ist eine der folgenden Optionen: *enable*, *disable* oder ein numerischer Wert.

Option	Beschreibung
enable	Aktiviert den oberen kritischen Schwellenwert für den angegebenen Umgebungssensor.
disable	Deaktiviert den oberen kritischen Schwellenwert für den angegebenen Umgebungssensor.
Ein numerischer Wert	Legt einen Wert für den oberen kritischen Schwellenwert des angegebenen Umgebungssensors fest und aktiviert diesen Schwellenwert.

Beispiel

Der folgende Befehl setzt den oberen kritischen Schwellenwert des Umgebungstemperatursensors mit der ID Nummer 2 auf 40 Grad Celsius. Er aktiviert darüber hinaus den oberen kritischen Schwellenwert, wenn er noch nicht aktiviert wurde.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Einstellen der oberen Warngrenze des Sensors

Diese Befehlssyntax konfiguriert die obere Warngrenze eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <Option> ist eine der folgenden Optionen: *enable*, *disable* oder ein numerischer Wert.

Option	Beschreibung
enable	Aktiviert die obere Warngrenze für den angegebenen Umgebungssensor.
disable	Deaktiviert die obere Warngrenze für den angegebenen Umgebungssensor.
Ein numerischer Wert	Legt einen Wert für die obere Warngrenze des angegebenen Umgebungssensors fest und aktiviert diesen Schwellenwert.

Beispiel

Der folgende Befehl aktiviert die obere Warngrenze des Umgebungstemperatursensors mit der ID Nummer 4.

```
config:#   sensor externalsensor 4 temperature upperWarning enable
```

Einstellen der unteren Warngrenze des Sensors

Diese Befehlssyntax konfiguriert den unteren kritischen Schwellenwert eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <Option> ist eine der folgenden Optionen: *enable*, *disable* oder ein numerischer Wert.

Option	Beschreibung
enable	Aktiviert den unteren kritischen Schwellenwert für den angegebenen Umgebungssensor.
disable	Deaktiviert den unteren kritischen Schwellenwert für den angegebenen Umgebungssensor.
Ein numerischer Wert	Legt einen Wert für den unteren kritischen Schwellenwert des angegebenen Umgebungssensors fest und aktiviert diesen Schwellenwert.

Beispiel

Der folgende Befehl setzt den unteren kritischen Schwellenwert des Umgebungsfeuchtigkeitssensors mit der ID Nummer 1 auf 15 %. Er aktiviert darüber hinaus den unteren kritischen Schwellenwert, wenn er noch nicht aktiviert wurde.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Einstellen der unteren Warngrenze des Sensors

Diese Befehlssyntax konfiguriert die untere Warngrenze eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <Option> ist eine der folgenden Optionen: *enable*, *disable* oder ein numerischer Wert.

Option	Beschreibung
enable	Aktiviert die untere Warngrenze für den angegebenen Umgebungssensor.
disable	Deaktiviert die untere Warngrenze für den angegebenen Umgebungssensor.
Ein numerischer Wert	Legt einen Wert für die unteren Warngrenze des angegebenen Umgebungssensors fest und aktiviert diese Grenze.

Beispiel

Der folgende Befehl deaktiviert die untere Warngrenze des Umgebungsfeuchtigkeitssensors mit der ID Nummer 3.

```
config:#   sensor externalsensor 3 humidity lowerWarning disable
```

Einstellen der Deassertion-Hysterese eines Sensors

Diese Befehlssyntax konfiguriert den Wert für die Deassertion-Hysterese eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

  Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <value> ist ein numerischer Wert, welcher der Hysterese für den angegebenen Umgebungssensor zugewiesen wird. Weitere Informationen zur Funktion der Deassertionshysterese finden Sie unter ***Was ist Deassertionshysterese?*** (auf Seite 189).

Beispiel

Der folgende Befehl setzt die Deassertion-Hysterese des Umgebungstemperatursensors mit der ID Nummer 4 auf 2 Grad Celsius. Das heißt, dass die Temperatur mindestens 2 Grad Celsius unter den oberen Schwellenwert fallen oder mindestens 2 Grad Celsius über den unteren Schwellenwert steigen muss, bevor eine Deassertion für die Schwellenwertunterschreitung bzw. -überschreitung durchgeführt wird.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Einstellen des Assertionszeitlimits eines Sensors

Diese Befehlssyntax konfiguriert den Wert für das Assertionszeitlimit eines numerischen Umgebungssensors.

```
config:#   sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

Variablen:

- <n> ist die ID des Umgebungssensors, den Sie konfigurieren möchten. Die ID-Nummer wird zugewiesen und in der EMX-Webschnittstelle angezeigt. Der Wert ist eine Ganzzahl zwischen 1 und 16.
- <Sensortyp> bezeichnet einen der folgenden Sensortypen: *temperature* (Temperatur), *humidity, airPressure oder air Flow* (Luftfeuchtigkeit, Luftdruck oder Luftstrom).

  Hinweis: Wenn der angegebene Sensortyp nicht mit dem Typ des angegebenen Umgebungssensors übereinstimmt, wird folgende Fehlermeldung angezeigt: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)" (Angegebener Sensortyp 'XXX' entspricht nicht dem Sensortyp (<sensortype>), wobei XXX der angegebenen Sensortyp und <sensortype> der korrekte Sensortyp ist.

- <value> ist ein numerischer Wert bei Messungen, welcher dem Assertionszeitlimit für den angegebenen Umgebungssensor zugewiesen wird. Siehe ***Was ist das Assertionszeitlimit?*** (auf Seite 190)

Beispiel

Der folgende Befehl setzt das Assertionszeitlimit des Umgebungstemperatursensors mit der ID Nummer 3 auf 4 Messungen. Dies bedeutet, dass mindestens 4 aufeinanderfolgende Messungen einen bestimmten Stromstärkenschwellenwert überschreiten müssen, bevor dieses Ereignis einer Schwellenwertüberschreitung bestätigt wird.

```
config:#   sensor externalsensor 3 temperature assertionTimeout 4
```

Befehle zur Benutzerkonfiguration

Die meisten Befehle zur Benutzerkonfiguration mit Ausnahme des Befehls zur Kennwortänderung beginnen mit *user*.

Erstellen von Benutzerprofilen

Diese Befehlssyntax erstellt ein neues Benutzerprofil.

```
config:#   user create <name> <option> <roles>
```

Nachdem der Befehl zum Erstellen eines Benutzers durchgeführt wurde, werden Sie von der EMX-Einheit aufgefordert, dem neu erstellten Benutzer ein Kennwort zuzuweisen. Gehen Sie anschließend wie folgt vor:

1. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
2. Geben Sie das Kennwort zur Bestätigung noch einmal ein, und drücken Sie die Eingabetaste.

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die <name>-Variable DARF KEINE Leerzeichen enthalten.
- <Option> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert das neu erstellte Benutzerprofil.
disable	Deaktiviert das neu erstellte Benutzerprofil.

- <roles> (Benutzerfunktion) ist eine Benutzerfunktion oder eine List durch Kommas getrennter Benutzerfunktionen, die dem angegebenen Benutzerprofil zugewiesen sind.

Beispiel

Der folgende Befehl erstellt ein neues Benutzerprofil und legt zwei Parameter für den neuen Benutzer fest.

```
config:#   user create May enable admin
```

Ergebnisse:

- Das neue Benutzerprofil "May" wird erstellt.
- Das neue Benutzerprofil wird aktiviert.
- Dem neuen Benutzerprofil wird die Rolle (Benutzerfunktion) **admin** zugewiesen.

Ändern von Benutzerprofilen

Ein Benutzerprofil enthält verschiedene Parameter, die Sie ändern können.

Tipp: Sie können alle Befehle kombinieren, um die Parameter eines bestimmten Benutzerprofils gleichzeitig zu ändern. Siehe **Multi-Befehlssyntax** *(auf Seite 330).*

Ändern eines Benutzerkennworts

Mit dieser Befehlssyntax können Sie das Kennwort eines bestehenden Benutzers ändern, wenn Sie über Administratorrechte verfügen.

```
config:#   user modify <name> password
```

Nachdem Sie den obigen Befehl ausgeführt haben, werden Sie von EMX zur Eingabe eines neuen Kennworts aufgefordert. Gehen Sie anschließend wie folgt vor:

1. Geben Sie ein neues Kennwort ein, und drücken Sie die Eingabetaste.
2. Geben Sie das neue Kennwort zur Bestätigung noch einmal ein, und drücken Sie die Eingabetaste.

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.

Beispiel

Im Folgenden wird beschrieben, wie Sie das Kennwort für den Benutzer "May" ändern.

1. Prüfen Sie, ob Sie den Konfigurationsmodus aufgerufen haben. Siehe ***Aufrufen des Konfigurationsmodus*** (auf Seite 240).
2. Geben Sie den folgenden Befehl ein, um das Kennwort für das Benutzerprofil "May" zu ändern.

   ```
   config:#   user modify May password
   ```
3. Geben Sie nach entsprechender Aufforderung ein neues Kennwort ein, und drücken Sie die Eingabetaste.
4. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.

5. Wenn die Kennwortänderung erfolgreich war, wird config:# angezeigt.

Ändern der persönlichen Daten eines Benutzers

Sie können die persönlichen Daten eines Benutzers, einschließlich vollständiger Name, Telefonnummer und E-Mail-Adresse des Benutzers, ändern.

Verwenden Sie diese Befehlssyntax, um den vollständigen Namen eines Benutzers zu ändern:

```
config:#   user modify <name> fullName "<full_name>"
```

Verwenden Sie diese Befehlssyntax, um die Telefonnummer eines Benutzers zu ändern:

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

Verwenden Sie diese Befehlssyntax, um die E-Mail-Adresse eines Benutzers zu ändern:

```
config:#   user modify <name> eMailAddress <email_address>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <full_name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die Variable <full_name> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.
- <phone_number> ist die Telefonnummer, unter der der angegebene Benutzer erreichbar ist. Die Variable <phone_number> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.
- <email_address> ist die E-Mail-Adresse des angegebenen Benutzers.

Tipp: Sie können alle Befehle kombinieren, um die Parameter eines bestimmten Benutzerprofils gleichzeitig zu ändern. Siehe **Multi-Befehlssyntax** *(auf Seite 330).*

Beispiel

Der folgende Befehl ändert zwei Parameter des Benutzerprofils "May":

```
config:#   user modify May fullName "May Turner" telephoneNumber 123-4567
```

Ergebnisse:

- Als vollständiger Name für "May" wurde "May Turner" angegeben.
- Die Telefonnummer ist mit 123-4567 angegeben.

Aktivieren oder Deaktivieren eines Benutzerprofils

Diese Befehlssyntax aktiviert oder deaktiviert ein Benutzerprofil. Ein Benutzer kann sich nur beim EMX-Gerät anmelden, nachdem sein Benutzerprofil aktiviert wurde.

```
config:#   user modify <name> enabled <option>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Aktiviert das angegebene Benutzerprofil.
false	Deaktiviert das angegebene Benutzerprofil.

Beispiel

Der folgende Befehl aktiviert das Benutzerprofil "May".

```
config:#   user modify May enabled true
```

Erzwingen einer Kennwortänderung

Diese Befehlssyntax legt fest, ob eine Kennwortänderung erzwungen wird, wenn sich ein Benutzer das nächste Mal mit dem angegebenen Benutzerprofil anmeldet.

```
config:#    user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <Option> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Bei der nächsten Anmeldung des Benutzers wird eine Kennwortänderung erzwungen.
false	Bei der nächsten Anmeldung des Benutzers wird keine Kennwortänderung erzwungen.

Beispiel

Der folgende Befehl erzwingt eine Kennwortänderung, wenn sich der Benutzer "May" das nächste Mal anmeldet.

```
config:#    user modify May forcePasswordChangeOnNextLogin true
```

Ändern der SNMPv3-Einstellungen

Zum Ändern der SNMPv3-Parameter eines bestimmten Benutzerprofils gibt es verschiedene Befehle. Sie können alle folgenden Befehle kombinieren, um die SNMPv3-Parameter gleichzeitig zu ändern. Siehe ***Multi-Befehlssyntax*** (auf Seite 330).

So aktivieren oder deaktivieren Sie den SNMP-v3-Zugriff auf EMX für den angegebenen Benutzer:

```
config:#    user modify <name> snmpV3Access <option1>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option1> ist eine der folgenden Optionen: *enable* oder *disable*.

Option	Beschreibung
enable	Aktiviert die SNMP-v3-Zugriffsberechtigung für den angegebenen Benutzer.
disable	Deaktiviert die SNMP-v3-Zugriffsberechtigung für den angegebenen Benutzer.

So legen Sie die Sicherheitsebene fest:

```
config:#    user modify <name> securityLevel <option2>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option2> ist eine der folgenden Optionen: *noAuthNoPriv*, *authNoPriv* oder *authPriv*.

Option	Beschreibung
noAuthNoPriv	Keine Authentifizierung und kein exklusiver Zugriff.
authNoPriv	Authentifizierung und kein exklusiver Zugriff.
authPriv	Authentifizierung und exklusiver Zugriff.

So legen Sie fest, ob der Authentifizierungsschlüssel mit dem Kennwort identisch ist:

```
config:#    user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option3> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Der Authentifizierungsschlüssel ist mit dem Kennwort identisch.
false	Der Authentifizierungsschlüssel ist nicht mit dem Kennwort identisch.

So legen Sie den Authentifizierungsschlüssel fest:

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <authentication_passphrase> ist ein als Authentifizierungsschlüssel verwendeter String mit bis zu 32 druckbaren ASCII-Zeichen.

So legen Sie fest, ob der Authentifizierungsschlüssel für den exklusiven Zugriff mit dem Authentifizierungsschlüssel identisch ist:

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option4> ist eine der folgenden Optionen: *true* oder *false*.

Option	Beschreibung
true	Der Authentifizierungsschlüssel für den exklusiven Zugriff ist mit dem Authentifizierungsschlüssel identisch.
false	Der Authentifizierungsschlüssel für den exklusiven Zugriff ist nicht mit dem Authentifizierungsschlüssel identisch.

So legen Sie den Authentifizierungsschlüssel für den exklusiven Zugriff fest:

```
config:#    user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <privacy_passphrase> ist ein als Authentifizierungsschlüssel für den exklusiven Zugriff verwendeter String mit bis zu 32 druckbaren ASCII-Zeichen.

So legen Sie das Authentifizierungsprotokoll fest:

```
config:#    user modify <name> authenticationProtocol <option5>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option5> ist eine der folgenden Optionen: *MD5* oder *SHA-1*.

Option	Beschreibung
MD5	Das MD5-Authentifizierungsprotokoll wird angewendet.
SHA-1	Das SHA-1-Authentifizierungsprotokoll wird angewendet.

So legen Sie das Protokoll für den exklusiven Zugriff fest:

```
config:#    user modify <name> privacyProtocol <option6>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option6> ist eine der folgenden Optionen: *DES* oder *AES-128*.

Option	Beschreibung
DES	Das DES-Protokoll für den exklusiven Zugriff wird angewendet.

Option	Beschreibung
AES-128	Das AES-128-Protokoll für den exklusiven Zugriff wird angewendet.

Beispiel

Der folgende Befehl legt drei SNMPv3-Parameter des Benutzers "May" fest.

```
config:#   user modify May snmpV3Access enable securityLevel authNoPriv
           userPasswordAsAuthenticationPassPhrase true
```

Ergebnisse:

- Die SNMPv3-Zugriffsberechtigung des Benutzers wird aktiviert.
- Die SNMPv3-Sicherheitsebene lautet "nur Authentifizierung, kein exklusiver Zugriff".
- Der Authentifizierungsschlüssel ist mit dem Kennwort des Benutzers identisch.

Ändern der Benutzerfunktionen

Diese Befehlssyntax ändert die Benutzerfunktionen (Rollen) eines bestimmten Benutzers.

```
config:#   user modify <name> roles <roles>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <roles> (Benutzerfunktion) ist eine Benutzerfunktion oder eine List durch Kommas getrennter Benutzerfunktionen, die dem angegebenen Benutzerprofil zugewiesen sind.

Beispiel

Der folgende Befehl weist dem Benutzer "May" zwei Benutzerfunktionen zu.

```
config:#   user modify May roles admin,tester
```

Ergebnisse:

- Der Benutzer "May" verfügt über alle Berechtigungen der Benutzerfunktionen "admin" und "tester".

Ändern der Maßeinheiten

Sie können die Maßeinheiten für die Temperatur, die Länge und den Druck für ein bestimmtes Benutzerprofil ändern. Verschiedene Befehle für Maßeinheiten lassen sich kombinieren, sodass Sie alle Maßeinheiten gleichzeitig festlegen können. Informationen zum Kombinieren aller Befehle finden Sie unter ***Multi-Befehlssyntax*** (auf Seite 330).

Hinweis: Die Änderung der Messeinheit gilt nur für die Webschnittstelle und die Befehlszeilenschnittstelle.

So richten Sie die bevorzugte Temperatureinheiten ein:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option1> ist eine der folgenden Optionen: *C* oder *F*.

Option	Beschreibung
C	Mit dieser Option wird die Temperatur in Celsius angezeigt.
F	Mit dieser Option wird die Temperatur in Fahrenheit angezeigt.

So richten Sie die bevorzugte Längeneinheiten ein:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option2> ist eine der folgenden Optionen: *meter* oder *feet*.

Option	Beschreibung
meter	Mit dieser Option wird die Länge oder Höhe in Meter angezeigt.
feet	Mit dieser Option wird die Länge oder Höhe in Fuß angezeigt.

So richten Sie die bevorzugte Einheit für den Druck ein:

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variablen:

- <name> ist der Name des Benutzers, dessen Einstellungen Sie ändern möchten.
- <option3> ist eine der folgenden Optionen: *pascal* oder *psi*.

Option	Beschreibung
pascal	Mit dieser Option wird der Druckwert in Pascal (Pa) angezeigt.
psi	Mit dieser Option wird der Druckwert in psi angezeigt.

Beispiel

Der folgende Befehl setzt alle Maßeinheiten für den Benutzer "May".

```
config:#    user modify May preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Ergebnisse:

- Die bevorzugte Temperatureinheit wird auf Fahrenheit festgelegt.
- Die bevorzugte Längeneinheit wird auf Fuß festgelegt.
- Die bevorzugte Einheit für den Druck wird auf psi festgelegt.

Angeben des öffentlichen SSH-Schlüssels

Wenn die Authentifizierung auf Basis eines SSH-Schlüssels aktiviert ist, geben Sie den öffentlichen SSH-Schlüssel für jedes Benutzerprofil wie nachfolgend beschrieben an.

So geben Sie den öffentlichen SSH-Schlüssel für einen bestimmten Benutzer an:

1. Geben Sie den Befehl für den öffentlichen SSH-Schlüssel wie unten gezeigt ein, und drücken Sie die Eingabetaste.

   ```
   config:#    user modify <Name> sshPublicKey
   ```

2. Sie werden aufgefordert, den Inhalt des öffentlichen SSH-Schlüssels einzugeben. Gehen Sie zur Eingabe des Inhalts folgendermaßen vor:

   a. Öffnen Sie den öffentlichen SSH-Schlüssel mit einem Texteditor.

   b. Kopieren Sie den gesamten Inhalt im Texteditor.

   c. Fügen Sie den Inhalt in das Terminal ein.

   d. Drücken Sie die Eingabetaste.

Tipp: Zum Entfernen eines vorhandenen öffentlichen SSH-Schlüssels drücken Sie einfach die Eingabetaste, ohne etwas einzugeben oder einzufügen, wenn Sie zur Eingabe des Inhalts aufgefordert werden.

Beispiel

In diesem Abschnitt wird gezeigt, wie Sie einen öffentlichen SSH-Schlüssel für den Benutzer "May" eingeben, wenn die Authentifizierung auf Basis eines öffentlichen SSH-Schlüssels aktiviert ist. Siehe ***Festlegen der SSH-Authentifizierungsmethode*** (auf Seite 265). Der Inhalt Ihres öffentlichen SSH-Schlüssels darf nicht mit dem in diesem Beispiel gezeigten Inhalt identisch sein.

So geben Sie den öffentlichen SSH-Schlüssel für den Benutzer "May" an:

1. Vergewissern Sie sich, dass Sie sich im Konfigurationsmodus befinden. Siehe ***Aufrufen des Konfigurationsmodus*** (auf Seite 240).
2. Geben Sie den folgenden Befehl ein, und drücken Sie die Eingabetaste.

   ```
   config:#   user modify May sshPublicKey
   ```

1. Sie werden aufgefordert, den Inhalt des öffentlichen SSH-Schlüssels einzugeben.
2. Öffnen Sie den öffentlichen SSH-Schlüssel mit einem Texteditor. Der Inhalt des öffentlichen SSH-Schlüssels müsste ungefähr wie folgt aussehen.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDLZMx/ETBqjczWo0uU6JHZ54H7PwIoHyAa
OdeKdCq8i0h59p1VVa6vS4agObxMU8FjHIZ0uQSLknTjWw3wy358BpJVYmyz8HlTOm
QBR59VvIrSjn77cI7U8DbYQOVgqm8NvFami1Fbd7yX/pMXikeSXZCxP4QtonDvqgZ36l
vjQ== May@raritan.com
```

3. Markieren und kopieren Sie den gesamten Inhalt des öffentlichen SSH-Schlüssels.
4. Fügen Sie den Inhalt in das Terminal ein.
5. Drücken Sie die Eingabetaste.

Löschen von Benutzerprofilen

Diese Befehlssyntax löscht ein bestehendes Benutzerprofil.

```
config:#   user delete <name>
```

Beispiel

Der folgende Befehl löscht das Benutzerprofil "May".

```
config:#   user delete May
```

Ändern des eigenen Kennworts

Jeder Benutzer kann sein eigenes Kennwort mit dieser Befehlssyntax ändern, wenn er/sie über die Berechtigung "Eigenes Kennwort ändern" verfügt. Beachten Sie, dass dieser Befehl nicht mit *user* beginnt.

```
config:#   password
```

Nachdem dieser Befehl ausgeführt wurde, fordert die EMX-Einheit Sie auf, das aktuelle und das neue Kennwort einzugeben.

Wichtig: Nachdem das Kennwort erfolgreich geändert wurde, tritt das neue Kennwort sofort in Kraft. Dies ist unabhängig davon, ob Sie den Befehl "apply" zum Speichern der Änderungen eingeben oder nicht.

Beispiel

So ändern Sie Ihr eigenes Kennwort:

1. Prüfen Sie, ob Sie den Konfigurationsmodus aufgerufen haben. Siehe ***Aufrufen des Konfigurationsmodus*** (auf Seite 240).
2. Geben Sie den folgenden Befehl ein, und drücken Sie die Eingabetaste.

   ```
   config:#   password
   ```
3. Geben Sie das bestehende Kennwort ein, und drücken Sie die Eingabetaste, wenn die folgende Eingabeaufforderung angezeigt wird.

   ```
   Current password (Aktuelles Kennwort):
   ```
4. Geben Sie das neue Kennwort ein, und drücken Sie die Eingabetaste, wenn die folgende Eingabeaufforderung angezeigt wird.

   ```
   Enter new password (Neues Kennwort eingeben):
   ```
5. Geben Sie das neue Kennwort zur Bestätigung erneut ein, und drücken Sie die Eingabetaste, wenn die folgende Eingabeaufforderung angezeigt wird.

   ```
   Re-type new password (Neues Kennwort erneut eingeben):
   ```

Befehle zur Konfiguration von Benutzerfunktionen

Ein Befehl zur Konfiguration einer Benutzerfunktion beginnt mit *role*.

Erstellen einer Benutzerfunktion

Diese Befehlssyntax erstellt eine neue Benutzerfunktion, wobei der Benutzerfunktion eine Liste von Berechtigungen zugewiesen wird, die durch Strichpunkt voneinander getrennt sind.

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

Wenn eine bestimmte Berechtigung Argumente enthält, müssen die Argumente mit einem Doppelpunkt an diese Berechtigung angeschlossen werden.

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält.
- <privilege1>, <privilege2>, <privilege3> usw. sind Namen von Berechtigungen, die der Benutzerfunktion zugewiesen sind. Trennen Sie jede Berechtigung durch ein Semikolon. Siehe ***Alle Berechtigungen*** (auf Seite 317).
- <argument1>, <argument2> usw. sind Argumente, die für eine bestimmte Berechtigung festgelegt sind. Trennen Sie eine Berechtigung und dessen Argument durch einen Doppelpunkt.

Alle Berechtigungen

Diese Tabelle enthält alle Berechtigungen.

Berechtigung	Beschreibung
adminPrivilege	Administratorrechte
changeAssetStripConfiguration	Asset-Strip-Konfiguration ändern

Berechtigung	Beschreibung
changeAuthSettings	Authentifizierungseinstellungen ändern
changeDataTimeSettings	Datum-/Uhrzeiteinstellungen ändern
changeEmdConfiguration	EMD-Konfiguration ändern
changeEventSetup	Ereigniseinstellungen ändern
changeExternalSensorsConfiguration	Konfiguration externer Sensoren ändern
changeLhxConfiguration	LHX-Konfiguration ändern
changeNetworkSettings	Netzwerkeinstellungen ändern
changePassword	Eigenes Kennwort ändern
changeSecuritySettings	Sicherheitseinstellungen ändern
changeSnmpSettings	SNMP-Einstellungen ändern
changeUserSettings	Lokale Benutzerverwaltung ändern
changeWebcamSettings	Webcam-Konfiguration ändern
clearLog	Lokales Ereignisprotokoll löschen
firmwareUpdate	Firmware Update (Firmware-Aktualisierung)
performReset	Zurücksetzen (Warmstart)
viewEventSetup	Ereigniseinstellungen anzeigen
viewLog	Lokales Ereignisprotokoll anzeigen
viewSecuritySettings	Sicherheitseinstellungen anzeigen
viewSnmpSettings	SNMP-Einstellungen anzeigen
viewUserSettings	Lokale Benutzerverwaltung anzeigen
viewWebcamSettings	Webcam-Bilder und -Konfiguration anzeigen

Beispiel

Der folgende Befehl erstellt eine neue Benutzerfunktion und weist ihr Berechtigungen zu.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Ergebnisse:

- Es wird eine neue Benutzerfunktion "tester" erstellt.
- Der Benutzerfunktion werden zwei Berechtigungen zugewiesen: firmwareUpdate (Firmwareaktualisierung) und viewEventSetup (Ereigniseinstellungen anzeigen).

Ändern von Benutzerfunktionen

Sie können verschiedene Parameter einer bestehenden Benutzerfunktion, einschließlich ihrer Berechtigungen, ändern.

So ändern Sie die Beschreibung einer Benutzerfunktion:

```
config:#   role modify <name> description <description>
```

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält.
- <description> ist eine Beschreibung mit alphanumerischen Zeichen. Die Variable <description> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.

So fügen Sie einer bestimmten Benutzerfunktion weitere Berechtigungen hinzu:

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

Wenn eine bestimmte Berechtigung Argumente umfasst, fügen Sie einen Doppelpunkt und das bzw. die Argument(e) hinter der Berechtigung hinzu.

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält.
- <privilege1>, <privilege2>, <privilege3> usw. sind Namen von Berechtigungen, die der Benutzerfunktion zugewiesen sind. Trennen Sie jede Berechtigung durch ein Semikolon. Siehe ***Alle Berechtigungen*** (auf Seite 317).
- <argument1>, <argument2> usw. sind Argumente, die für eine bestimmte Berechtigung festgelegt sind. Trennen Sie eine Berechtigung und dessen Argument durch einen Doppelpunkt.

So entfernen Sie bestimmte Berechtigungen aus einer Benutzerfunktion:

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

Wenn eine bestimmte Berechtigung Argumente umfasst, fügen Sie einen Doppelpunkt und das bzw. die Argument(e) hinter der Berechtigung hinzu.

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Hinweis: Beim Entfernen von Berechtigungen aus einer Benutzerfunktion müssen Sie sicherstellen, dass die angegebenen Berechtigungen und Argumente (sofern vorhanden) genau mit denen übereinstimmen, die der Benutzerfunktion zugewiesen sind. Der Befehl kann angegebene Berechtigungen, die nicht verfügbar sind, sonst nicht entfernen.

Variablen:

- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält.
- <privilege1>, <privilege2>, <privilege3> usw. sind Namen von Berechtigungen, die der Benutzerfunktion zugewiesen sind. Trennen Sie jede Berechtigung durch ein Semikolon. Siehe ***Alle Berechtigungen*** (auf Seite 317).
- <argument1>, <argument2> usw. sind Argumente, die für eine bestimmte Berechtigung festgelegt sind. Trennen Sie eine Berechtigung und dessen Argument durch einen Doppelpunkt.

Beispiel

Der folgende Befehl ändert die Berechtigungen der Benutzerfunktion "tester".

```
config:#    role modify tester addPrivileges changeAuthSettings removePrivileges
            firmwareUpgrade
```

Ergebnisse:

- Die Berechtigung "changeAuthSettings" (Authentifizierungseinstellungen ändern) wird der Benutzerfunktion hinzugefügt.
- Die Berechtigung "firmwareUpgrade" (Firmware-Upgrade) wird aus der Benutzerfunktion entfernt.

Löschen einer Benutzerfunktion

Diese Befehlssyntax löscht eine bestehende Benutzerfunktion.

```
config:#    role delete <name>
```

Beispiel

Der folgende Befehl löscht eine vorhandene Benutzerfunktion.

```
config:#   role delete tester
```

Befehle zur Assetverwaltung

Sie können die Einstellungen für den angeschlossenen Assetsensor (sofern vorhanden) oder die Einstellungen für die LEDs des Assetsensors mithilfe der CLI-Befehle ändern.

Verwaltung des Assetsensors

Ein Befehl für die Konfiguration der Assetsensorverwaltung beginnt mit `assetStrip`.

Benennen eines Assetsensors

Diese Befehlssyntax benennt einen Assetsensor oder ändert den Namen eines Assetsensors, der an das EMX-Gerät angeschlossen ist.

```
config:#   assetStrip <n> name "<name>"
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die Variable <name> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.

Beispiel

Diese Befehlssyntax benennt einen Assetsensor oder ändert den Namen eines Assetsensors, der an das EMX-Gerät angeschlossen ist.

```
config:#   assetStrip 1 name "Red Rack"
```

Angeben der Anzahl an Rackeinheiten

Diese Befehlssyntax gibt die Gesamtanzahl der Rackeinheiten an einem Assetsensor an, der an das EMX-Gerät angeschlossen ist.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Hinweis: Bei einem Raritan-Assetsensor bezieht sich eine Rackeinheit auf einen Tag-Port.

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <number> ist die Gesamtanzahl der Rackeinheiten, die am angeschlossenen Assetsensor verfügbar sind. Es kann ein Wert von 8 bis 64 angegeben werden.

Beispiel

Der folgende Befehl gibt die Gesamtanzahl der Rackeinheiten an Assetsensor 1 mit 48 Rackeinheiten an.

```
config:#   assetStrip 1 numberOfRackUnits 48
```

Angeben des Nummerierungsmodus für Rackeinheiten

Diese Befehlssyntax gibt den Nummerierungsmodus der Rackeinheiten an einem Assetsensor an, der an das EMX-Gerät angeschlossen ist. Der Nummerierungsmodus ändert die Nummern der Rackeinheiten.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <mode> ist einer der folgenden Nummerierungsmodi: *topDown* oder *bottomUp*.

Modus	Beschreibung
topDown	Die Rackeinheiten sind in aufsteigender Reihenfolge von oben nach unten nummeriert.
bottomUp	Die Rackeinheiten sind in absteigender Reihenfolge von oben nach unten nummeriert.

Beispiel

Mit dem folgenden Befehl werden die Rackeinheiten von Assetsensor 1 in aufsteigender Reihenfolge nummeriert, ausgehend von der Einheit, die dem RJ-45-Anschluss des Assetsensors am nächsten liegt, bis zu der Einheit, die am weitesten davon entfernt ist. Das bedeutet, dass der Rackeinheit, die dem RJ-45-Anschluss am nächsten ist, die Nummer 1 zugewiesen wird.

```
config:#   assetStrip 1 rackUnitNumberingMode topDown
```

Angeben der Nummerierungsverschiebung für Rackeinheiten

Diese Befehlssyntax gibt die Anfangsnummer der Rackeinheiten an einem Assetsensor an, der an das EMX-Gerät angeschlossen ist.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <number> ist die Anfangsnummer beim Nummerieren von Rackeinheiten am angeschlossenen Assetsensor. Dieser Wert ist eine ganze Zahl.

Beispiel

Der folgende Befehl gibt an, dass die Anfangsnummer für Rackeinheiten des Assetsensors 1 die Nummer 5 ist. Das heißt, dass die Rackeinheiten von der ersten bis zur letzten Rackeinheit am Assetsensor 1 mit 5, 6, 7 usw. nummeriert werden.

```
config:#   assetStrip 1 rackUnitNumberingOffset 5
```

Angeben der Ausrichtung des Assetsensors

Diese Befehlssyntax gibt die Ausrichtung der Assetsensoren an, die an das EMX-Gerät angeschlossen sind. Sie brauchen diesen Befehl normalerweise nicht auszuführen, es sei denn, die Assetsensoren besitzen KEINEN Neigungssensor, sodass die EMX-Einheit die Ausrichtung der Assetsensoren nicht erkennen kann.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <orientation> ist eine der folgenden Optionen: *topConnector* oder *bottomConnector*.

Ausrichtung	Beschreibung
topConnector	Diese Option gibt an, dass der Assetsensor so montiert ist, dass sich der RJ-45-Anschluss oben befindet.
bottomConnector	Diese Option gibt an, dass der Assetsensor so montiert ist, dass sich der RJ-45-Anschluss unten befindet.

Beispiel

Der folgende Befehl gibt an, dass sich der RJ-45-Anschluss des Assetsensors 1 oben befindet.

```
config:#   assetStrip 1 assetStripOrientation topConnector
```

Konfiguration der Rackeinheiten

Bei einem Raritan-Assetsensor bezieht sich eine Rackeinheit auf einen Tag-Port. Ein Befehl zur Konfiguration von Rackeinheiten beginnt mit `rackUnit`.

Benennen einer Rackeinheit

Diese Befehlssyntax weist der angegebenen Rackeinheit am angegebenen Assetsensor einen Namen zu oder ändert den Namen.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist die Indexnummer der gewünschten Rackeinheit. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.
- <name> ist ein String, der maximal 32 druckbare ASCII-Zeichen enthält. Die Variable <name> muss in Anführungszeichen stehen, wenn Leerzeichen enthalten sind.

Beispiel

Der folgende Befehl weist der Rackeinheit mit der Indexnummer 25 an Assetsensor 1 den Namen "Linux server" zu.

```
config:#   rackUnit 1 25 name "Linux server"
```

Festlegen des LED-Betriebsmodus

Diese Befehlssyntax legt fest, ob eine bestimmte Rackeinheit am angegebenen Assetsensor die globalen LED-Farbeinstellungen verwendet.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist die Indexnummer der gewünschten Rackeinheit. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.
- <mode> ist einer der folgenden LED-Modi: *automatic* oder *manual*.

Modus	Beschreibung
automatic	Mit dieser Option verwendet die LED der angegebenen Rackeinheit die globalen LED-Farbeinstellungen. Siehe Globale Einstellungen für LED-Farben. Dies ist die Standardeinstellung.
manual	Diese Option ermöglicht die Auswahl einer anderen LED-Farbe und eines anderen LED-Modus für die angegebene Rackeinheit. Informationen zum Festlegen unterschiedlicher LED-Einstellungen bei Auswahl dieser Option finden Sie unter ***Festlegen einer LED-Farbe für eine Rackeinheit*** (auf Seite 328) und ***Festlegen eines LED-Modus für eine Rackeinheit*** (auf Seite 329).

Beispiel

Der folgende Befehl erlaubt, dass die Rackeinheit mit der Indexnummer 25 an Assetsensor 1 eine andere LED-Farbe und einen anderen LED-Modus hat.

```
config:#   rackUnit 1 25 LEDOperationMode manual
```

Festlegen der LED-Farbe für "nicht angeschlossen"

Diese Befehlssyntax legt die LED-Farbe für alle Rackeinheiten an den angeschlossenen Assetsensoren fest, um das Fehlen eines angeschlossenen Asset-Tag anzugeben.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Festlegen einer LED-Farbe für eine Rackeinheit

Diese Befehlssyntax legt die LED-Farbe für eine bestimmte Rackeinheit am angegeben Assetsensor fest. Sie müssen die LED-Farbe einer Rackeinheit nur festlegen, wenn der LED-Betriebsmodus dieser Rackeinheit auf "manuell" gesetzt wurde.

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist die Indexnummer der gewünschten Rackeinheit. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.
- <color> ist der hexadezimale RGB-Wert einer Farbe im HTML-Format. Die <color>-Variable liegt zwischen #000000 und #FFFFFF.

Hinweis: Die LED-Farbeinstellung einer Rackeinheit überschreibt die globale LED-Farbeinstellung. Siehe Globale Einstellungen für LED-Farben.

Beispiel

Der folgende Befehl legt die LED-Farbe der Rackeinheit mit der Indexnummer 25 am Assetsensor 1 auf ROSA (d. h. FF00FF) fest.

```
config:#   rackUnit 1 25 LEDColor #FF00FF
```

Festlegen eines LED-Modus für eine Rackeinheit

Diese Befehlssyntax legt den LED-Modus für eine bestimmte Rackeinheit am angegeben Assetsensor fest. Sie müssen den LED-Modus einer Rackeinheit nur festlegen, wenn der LED-Betriebsmodus dieser Rackeinheit auf "manuell" gesetzt wurde.

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variablen:

- <n> ist die Nummer des FEATURE-Ports, an den der ausgewählte Assetsensor physisch angeschlossen ist. Für ein EMX-Gerät mit nur einem FEATURE-Port ist die Nummer immer 1.
- <rack_unit> ist die Indexnummer der gewünschten Rackeinheit. Die Indexnummer jeder Rackeinheit ist auf der Seite "Asset Strip" der Webschnittstelle verfügbar.
- <mode> ist einer der folgenden LED-Modi: *on*, *off*, *blinkSlow* oder *blinkFast*.

Modus	Beschreibung
on	Bei diesem Modus leuchtet die LED permanent.
off	Bei diesem Modus bleibt die LED permanent aus.
blinkSlow	Bei diesem Modus blinkt die LED langsam.
blinkFast	Bei diesem Modus blinkt die LED schnell.

Beispiel

Der folgende Befehl bewirkt, dass die LED der Rackeinheit mit der Indexnummer 25 am Assetsensor 1 schnell blinkt.

```
config:#   rackUnit 1 25 LEDMode blinkFast
```

Festlegen der Größe eines Verlaufspuffers

Diese Befehlssyntax ändert die Größe des Verlaufspuffers. Die Standardgröße ist 25.

```
config:#   history length <n>
```

Variablen:

- <n> ist eine ganze Zahl zwischen 1 und 250.
- Wenn Sie bei Verwendung des Befehls für die Variable <n> nichts angeben, wird der Verlaufspuffer standardmäßig auf 25 gesetzt.

Multi-Befehlssyntax

Zur Verkürzung der Konfigurationszeit können Sie verschiedene Konfigurationsbefehle in einem Befehl zusammenfassen und alle gleichzeitig ausführen.

Eine Multi-Befehlssyntax sieht wie folgt aus:

```
<Einstellung 1> <Wert 1> <Einstellung 2> <Wert 2>
<Einstellung 3> <Wert 3> ...
```

Beispiel 1 – Kombination aus IP-, Subnetzmaske- und Gateway-Parametern

Die folgende Multi-Befehlssyntax konfiguriert gleichzeitig IPv4-Adresse, Subnetzmaske und Gateway für die Netzwerkkonnektivität.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
           gateway 192.168.84.0
```

Ergebnisse:

- Die IP-Adresse wird auf 192.168.84.225 eingestellt.
- Die Subnetzmaske wird auf 255.255.255.0 eingestellt.
- Das Gateway wird auf 192.168.84.0 eingestellt.

Beispiel 2 – Kombination von SSID- und PSK-Parametern

Diese Multi-Befehlssyntax konfiguriert gleichzeitig die SSID- und die PSK-Parameter für die Drahtlosfunktion.

```
config:#    network wireless SSID myssid PSK encryp_key
```

Ergebnisse:

- Der SSID-Wert wird auf myssid gesetzt.
- Der PSK-Wert wird auf encryp_key gesetzt.

Beenden des Konfigurationsmodus

Sie können den Konfigurationsmodus sowohl mit dem Befehl "apply" als auch mit dem Befehl "cancel" verlassen. Der Unterschied besteht darin, dass "apply" alle im Konfigurationsmodus vorgenommenen Änderungen speichert, während "cancel" alle Änderungen verwirft.

Zum Beenden des Konfigurationsmodus verwenden Sie einen der beiden Befehle:

```
config:#    apply (Übernehmen)
```

-- ODER --

```
config:#    cancel (Abbrechen)
```

Die Eingabeaufforderung # wird angezeigt, nachdem Sie die Eingabetaste gedrückt haben, und weist darauf hin, dass Sie den Administratormodus aufgerufen haben.

Aufheben der Sperrung eines Benutzers

Wenn der Zugriff auf die EMX-Einheit für einen Benutzer gesperrt ist, können Sie die Sperrung dieses Benutzers an der lokalen Konsole aufheben.

So heben Sie die Sperrung eines Benutzers auf:

1. Melden Sie sich mit einem Terminalprogramm über eine lokale Verbindung bei der CLI-Schnittstelle an. Siehe ***Mit HyperTerminal*** (auf Seite 225).

2. Geben Sie bei der Eingabeaufforderung "Username" (Benutzername) `unblock` ein, und drücken Sie die Eingabetaste.

```
Username: unblock
```

3. Wenn die Eingabeaufforderung "Username to unblock" (Name des zu entsperrenden Benutzers) angezeigt wird, geben Sie den Anmeldenamen des Benutzers ein, dessen Sperrung aufgehoben werden soll, und drücken Sie die Eingabetaste.

```
Username to unblock:
```

4. Eine Meldung gibt an, dass die Sperrung des angegebenen Benutzers erfolgreich aufgehoben wurde.

Zurücksetzen der EMX-Einheit

Sie können das EMX-Gerät auf die werkseitigen Standardeinstellungen zurücksetzen oder mit den CLI-Befehlen neu starten.

Neustart des Geräts

Dieser Befehl startet das EMX-Gerät neu. Es erfolgt keine Rücksetzung auf die werkseitigen Standardeinstellungen.

So starten Sie das EMX-Gerät neu:

1. Vergewissern Sie sich, dass Sie den Administratormodus aufgerufen haben und die Eingabeaufforderung # angezeigt wird.
2. Geben Sie einen der folgenden Befehle ein, um das EMX-Gerät neu zu starten.

```
#      reset unit
```

-- ODER --

```
#      reset unit /y
```

3. Wenn Sie den Befehl in Schritt 2 ohne "`/y`" eingegeben haben, werden Sie aufgefordert, den Vorgang zu bestätigen. Geben Sie "y" ein, um das Zurücksetzen zu bestätigen.
4. Warten Sie, bis die Eingabeaufforderung "Username" (Benutzername) angezeigt wird, die darauf hinweist, dass das Zurücksetzen abgeschlossen ist.

Wiederherstellen der werksseitigen Standardeinstellungen

Dieser Befehl setzt alle Einstellungen des EMX-Geräts auf die werkseitigen Standardeinstellungen zurück.

Verwenden Sie einen der folgenden Befehle, um die Einstellungen von EMX zurückzusetzen:

```
#      reset factorydefaults
```

-- ODER --

```
#      reset factorydefaults /y
```

Weitere Informationen finden Sie unter Verwenden des CLI-Befehls.

Behebung von Netzwerkproblemen

Die EMX-Einheit bietet 4 Diagnosebefehle für die Behebung von Netzwerkproblemen: *nslookup*, *netstat*, *ping* und *traceroute*. Die Diagnosebefehle funktionieren wie die entsprechenden Linux-Befehle und können entsprechende Linux-Ausgaben erzeugen.

Aufrufen des Diagnosemodus

Die Diagnosebefehle funktionieren nur im Diagnosemodus.

So rufen Sie den Diagnosemodus auf:

1. Vergewissern Sie sich, dass Sie den Administratormodus aufgerufen haben und die Eingabeaufforderung # angezeigt wird.
2. Geben Sie `diag` ein, und drücken Sie die Eingabetaste. Die Eingabeaufforderung diag> wird angezeigt und weist darauf hin, dass Sie sich nun im Diagnosemodus befinden.
3. Sie können nun Diagnosebefehle für die Fehlerbehebung eingeben.

Diagnosebefehle

Die Syntax für Diagnosebefehle ist von Befehl zu Befehl unterschiedlich.

Abfragen der DNS-Server

Diese Befehlssyntax fragt die Internet Domain Name Server (DNS)-Informationen eines Netzwerkhosts ab.

```
diag>       nslookup <host>
```

Variablen:

- <host> ist der Name oder die IP-Adresse des Hosts, dessen DNS-Informationen Sie abfragen möchten.

Beispiel

Der folgende Befehl prüft die DNS-Informationen für den Host 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Anzeigen der Netzwerkverbindungen

Diese Befehlssyntax zeigt die Netzwerkverbindungen und/oder den Status von Ports an.

```
diag>       netstat <option>
```

Variablen:

- <Option> ist eine der folgenden Optionen: *ports* oder *connections*.

Option	Beschreibung
ports	Zeigt TCP/UDP-Ports an.
connections	Zeigt Netzwerkverbindungen an.

Beispiel

Der folgende Befehl zeigt die Serververbindungen zu Ihrem EMX-Gerät an.

```
diag>       netstat connections
```

Testen der Netzwerkkonnektivität

Diese Befehlssyntax sendet die Nachricht ICMP ECHO_REQUEST an einen Netzwerkhost, um dessen Netzwerkkonnektivität zu prüfen. Wenn die Ausgabe zeigt, dass der Host korrekt antwortet, ist die Netzwerkkonnektivität gut, andernfalls ist der Host ausgeschaltet oder nicht mit dem Netzwerk verbunden.

```
diag>       ping <host>
```

Variablen:

- <host> ist der Hostname oder die IP-Adresse, dessen/deren Netzwerkkonnektivität Sie prüfen möchten.

Optionen:

- Sie können eine oder alle der unten aufgeführten zusätzlichen Optionen im Befehl "ping" aufnehmen.

Optionen	Beschreibung
count <number1>	Bestimmt die Anzahl der zu sendenden Nachrichten. <number1> ist eine Ganzzahl.
size <number2>	Bestimmt die Paketgröße. <number2> ist eine Ganzzahl in Byte.
timeout <number3>	Bestimmt die Wartezeit vor der Zeitüberschreitung. <number3> ist eine Ganzzahl in Sekunden.

Der Befehl hat folgende Syntax, wenn er alle Optionen enthält:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Beispiel

Der folgende Befehl prüft die Netzwerkkonnektivität des Hosts 192.168.84.222, indem fünfmal die Nachricht ICMP ECHO_REQUEST an den Host gesendet wird.

```
diag>       ping 192.168.84.222 count 5
```

Verfolgen der Route

Diese Befehlssyntax verfolgt die Netzwerkroute zwischen Ihrem EMX-Gerät und einem Netzwerkhost.

```
diag>       traceroute <host>
```

Variablen:

- <host> ist der Name oder die IP-Adresse des Hosts, den Sie verfolgen möchten.

Beispiel

Der folgende Befehl zeigt das vorhandene Netzwerk-Routing für den Host 192.168.84.222 an.

```
diag>       traceroute 192.168.84.222
```

Beenden des Diagnosemodus

Mit dem folgenden Befehl verlassen Sie den Diagnosemodus:

```
diag>       exit
```

Die Eingabeaufforderung # wird angezeigt, nachdem Sie die Eingabetaste gedrückt haben, und weist darauf hin, dass Sie den Administratormodus aufgerufen haben.

Abfragen verfügbarer Parameter für einen Befehl

Wenn Sie sich nicht sicher sind, welche Befehle oder Parameter für einen bestimmten CLI-Befehlstyp verfügbar sind, können Sie diese über die CLI anzeigen, indem Sie ein Leerzeichen gefolgt von einem Fragezeichen am Ende des Befehls hinzufügen. Es wird eine Liste verfügbarer Parameter mit Beschreibungen angezeigt.

Nachfolgend finden Sie einige Abfragebeispiele.

- **Die Syntax zum Abfragen verfügbarer Parameter für den Befehl "show" lautet:**

```
#           show ?
```

- **Die Syntax für das Abfragen verfügbarer Netzwerkkonfigurationsparameter lautet:**

```
config:#    network ?
```

- **Die Syntax zum Abfragen verfügbarer Parameter für die Konfiguration von Benutzerfunktionen lautet:**

```
config:#    role ?
```

Abrufen vorheriger Befehle

Wenn Sie einen Befehl abrufen möchten, den Sie zuvor während derselben Verbindungssitzung eingegeben haben, drücken Sie auf der Tastatur auf den Pfeil nach oben (↑), bis der gewünschte Befehl angezeigt wird.

Automatisches Vervollständigen eines Befehls

Ein CLI-Befehl besteht immer aus mehreren Wörtern. Einige *eindeutige* CLI-Befehle, wie z. B. den Befehl "reset", können Sie leicht vervollständigen, indem Sie die Tabulator- oder Strg-Taste + i drücken, anstatt den gesamten Befehl Wort für Wort einzugeben.

- **So vervollständigen Sie einen eindeutigen Befehl automatisch:**

1. Geben Sie die ersten Buchstaben oder Wörter des Befehls ein. Geben Sie z. B. das erste Wort des Befehls "`reset factorydefaults`" ein, also `reset`.
2. Drücken Sie die Tabulator- oder Strg-Taste + i, bis der vollständige Befehl erscheint. Obwohl Sie nur ein Wort des Reset-Befehls eingegeben haben, erscheint nach Drücken der Tabulator- oder Strg-Taste + i der Rest des Befehls.

Abmelden bei der CLI

Nachdem Sie Ihre Aufgaben mit der CLI abgeschlossen haben, sollten Sie sich immer von der CLI abmelden, damit andere nicht darauf zugreifen können.

So melden Sie sich bei der CLI ab:

1. Vergewissern Sie sich, dass Sie den Administratormodus aufgerufen haben und die Eingabeaufforderung # angezeigt wird.
2. Geben Sie `exit` ein, und drücken Sie die Eingabetaste.

Wiederherstellen der werksseitigen Standardeinstellungen (CLI)

Die Befehlszeilenschnittstelle (CLI) bietet einen Reset-Befehl für das Wiederherstellen der werkseitigen Standardeinstellungen der EMX-Einheit. Weiter Informationen zu CLI finden Sie unter Verwenden der Befehlszeilenschnittstelle.

So setzen Sie das Gerät mit dem CLI-Befehl auf die werkseitigen Standardeinstellungen zurück:

1. Schließen Sie einen Computer an das EMX-Gerät an. Siehe ***Anschließen der EMX-Einheit an einen Computer*** (auf Seite 11).
2. Öffnen Sie in EMX über ein Terminalemulationsprogramm, wie HyperTerminal, Kermit oder PuTTY, ein Terminalfenster.
3. Melden Sie sich bei der CLI an, indem Sie den Benutzernamen "admin" und das zugehörige Kennwort eingeben. Siehe Schritt 4 von Erste Netzwerkkonfiguration.
4. Wenn die Systemeingabeaufforderung # angezeigt wird, geben Sie einen der folgenden Befehle ein, und drücken Sie die Eingabetaste.
5. Geben Sie Folgendes ein:

```
#    reset factorydefaults

ODER

#   reset factorydefaults /y
```

6. Warten Sie, bis die Eingabeaufforderung "Username" (Benutzername) angezeigt wird, die darauf hinweist, dass das Zurücksetzen abgeschlossen ist.
7. Wenn Sie den Befehl ohne "`/y`" eingegeben haben, werden Sie aufgefordert, den Vorgang zu bestätigen. Geben Sie "y" ein, um das Zurücksetzen zu bestätigen.

Anhang A Asset-Management bei Dominion PX

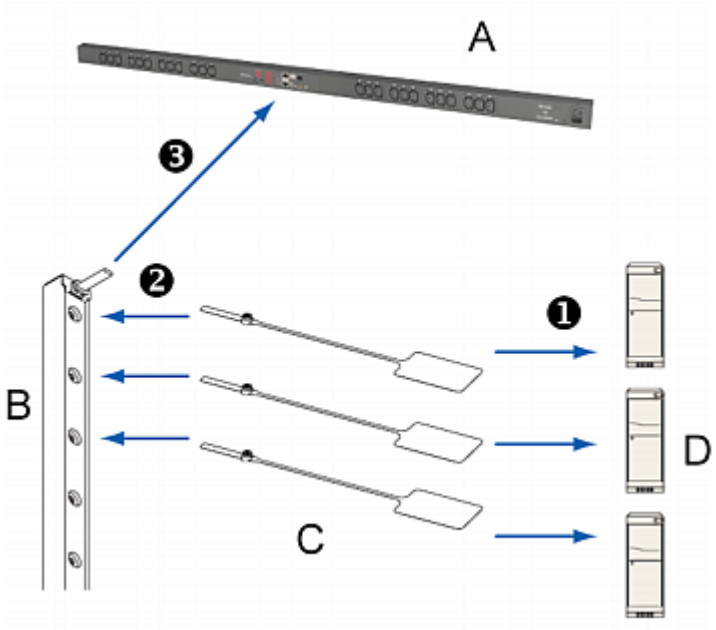
In diesem Kapitel

Übersicht.....339

Übersicht

Die PX2-Stromverteilungseinheit (PDU) von Raritan unterstützt auch Assetsensoren, sodass Sie IT-Geräte über die Webschnittstelle der Stromverteilungseinheit per Fernzugriff verfolgen können, während Sie den Stromzufuhrstatus der Stromverteilungseinheit überwachen. Nur PDUs, deren Modellname mit 'PX2' beginnt, unterstützen die Asset-Management-Funktion.

Wichtig: Üben Sie beim Umgang mit Assetsensoren, die miteinander verbunden sind, möglichst wenig Druck auf die Verbindungen zwischen den Assetsensoren aus, um einen Bruch der Verbindungsstelle zu vermeiden.



Buchstabe	Position
A	Dominion PX-Gerät

Buchstabe	Position
B	Asset-Sensoren
C	Asset-Tags
D	IT-Geräte, z. B. Server

So richten Sie ein Asset-Management-System ein:

1. Befestigen Sie das klebende Ende eines Asset-Tags an jedem IT-Gerät.
2. Stecken Sie den Stecker am anderen Ende jedes Asset-Tags in den entsprechenden Tag-Port am Asset-Sensor.
3. Schließen Sie die Asset-Sensor-Baugruppe am Rack wie folgt an das Dominion PX-Gerät an:
   a. Schließen Sie ein Ende des UTP-Kabels der Kategorie 5e/6 an den RJ-45-Anschluss am Assetsensor an.
   b. Schließen Sie das andere Ende des Kabels an den FEATURE-Port auf dem Dominion PX-Gerät an.

Weitere Informationen zum Dominion PX-Produkt finden Sie in der Dominion PX-Dokumentation, die mit dem Dominion PX-Gerät geliefert wird. Sie können diese Dokumentation im Bereich ***Firmware and Documentation*** (***http://www.raritan.com/support/firmware-and-documentation/***) (Firmware und Dokumentation) der Raritan-Website herunterladen. Oder: Sie können auf die Online-Hilfe des Produkts im Bereich "Product Online Help" (http://www.raritan.com/support/online-help/) zugreifen.

Anhang B Spezifikationen

In diesem Kapitel

Faktoren zur Höhenkorrektur (EMX) 341
Maximale Umgebungstemperatur für den Betrieb (EMX) 342
Pinbelegung des seriellen RS-232-Ports 342
RJ-12-Pin-Belegung 342
Pinbelegung des RS-485-Ports.....343

Faktoren zur Höhenkorrektur (EMX)

Wenn an Ihr Gerät ein Raritan-Differenzdrucksensor angeschlossen ist, kann die von Ihnen für das Gerät eingegebene Höhe über dem Meeresspiegel als Faktor zur Höhenkorrektur dienen. Das bedeutet, dass das Messergebnis des Differenzdrucksensors mit dem Korrekturfaktor multipliziert wird, um ein korrektes Ergebnis zu erhalten.

Die folgende Tabelle zeigt die Beziehung zwischen verschiedenen Höhen und den Korrekturfaktoren.

Höhe über Meeresspiegel (Meter)	Höhe über Meeresspiegel (Fuß)	Korrekturfaktor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Maximale Umgebungstemperatur für den Betrieb (EMX)

Die maximale Umgebungstemperatur für den Betrieb (TMA) des EMX-Geräts ist für alle Modelle gleich, unabhängig vom Zertifizierungsstandard (CE oder UL).

Spezifikation	Wert
Max. Umgebungstemperatur	60 Grad Celsius

Pinbelegung des seriellen RS-232-Ports

RS-232 – Pin-/Signaldefinition			
Pin-Nr.	Signal	Richtung	Beschreibung
1	DCD	Eingang	daten
2	RxD	Eingang	Datenempfang (eingehende Daten)
3	TxD	Ausgabe	Datenübertragung
4	DTR	Ausgabe	Datenterminal bereit
5	GND	—	Betriebserde
6	DSR	Eingang	Betriebsbereitschaft
7	RTS	Ausgabe	Sendeanforderung
8	CTS	Eingang	Sendebereit
9	RI	Eingang	Anrufsignal

RJ-12-Pin-Belegung

RJ-12 – Pin-/Signaldefinition			
Pin-Nr.	Signal	Richtung	Beschreibung
1	+12V	—	Power (500 mA, abgesichert)
2	GND	—	Betriebserde
3	—	—	—
4	—	—	—

RJ-12 – Pin-/Signaldefinition			
5	GND	—	Betriebserde
6	1-Wire		Verwendet für Feature-Port

Pinbelegung des RS-485-Ports

RS-485 – Pin-/Signaldefinition			
Pin-Nr.	Signal	Richtung	Beschreibung
1	—	—	—
2	—	—	—
3	D+	Bidirektional	Daten +
4	—	—	—
5	—	—	—
6	D-	Bidirektional	Daten -
7	—	—	—
8	—	—	—

Anhang C Veranschaulichung der LDAP-Konfiguration

Dieser Abschnitt enthält ein LDAP-Beispiel, welches den Konfigurationsvorgang mit Microsoft Active Directory® (AD) demonstriert. Für die Konfiguration der LDAP-Authentifizierung sind vier wesentliche Schritte auszuführen:

a. Festlegen der Benutzerkonten und Gruppen für die EMX-Einheit

b. Erstellen der Benutzergruppen für die EMX-Einheit auf dem AD-Server

c. Konfigurieren der LDAP-Authentifizierung auf dem EMX-Gerät

d. Konfigurieren von Rollen auf dem EMX-Gerät

In diesem Kapitel

Schritt A. Festlegen der Benutzerkonten und Gruppen 344
Schritt B. Konfigurieren der Benutzergruppen auf dem AD-Server 345
Schritt C. Konfigurieren der LDAP-Authentifizierung auf dem EMX-Gerät 346
Schritt D. Konfigurieren der Benutzergruppen auf dem EMX-Gerät..... 349

Schritt A. Festlegen der Benutzerkonten und Gruppen

Bestimmen Sie die Benutzerkonten und Gruppen, die auf die EMX-Einheit zugreifen dürfen. In diesem Beispiel werden wir zwei Benutzergruppen mit verschiedenen Berechtigungen erstellen. Jede Gruppe besteht aus zwei Benutzerkonten, die auf dem AD-Server verfügbar sind.

Benutzergruppen	Benutzerkonten (Mitglieder)
EMX_User	usera
	emxuser2
EMX_Admin	userb
	emxuser

Gruppenberechtigungen:

- Die Gruppe "EMX_User" verfügt lediglich über Leseberechtigung.
- Die Gruppe "EMX_Admin" verfügt über uneingeschränkte Systemberechtigungen.

Schritt B. Konfigurieren der Benutzergruppen auf dem AD-Server

Sie müssen die Gruppen für die EMX-Einheit auf dem AD-Server erstellen und anschließend die jeweiligen Benutzer zu Mitgliedern dieser Gruppen erklären.

Bei dieser Veranschaulichung gehen wir von Folgendem aus:

- Die Gruppen für das EMX-Gerät heißen *EMX_Admin* und *EMX_User*.
- Die Benutzerkonten *emxuser*, *emxuser2*, *usera* und *userb* sind bereits auf dem AD-Server vorhanden.

So konfigurieren Sie Benutzergruppen auf dem AD-Server:

1. Erstellen Sie auf dem AD-Server neue Gruppen – *EMX_Admin* und *EMX_User*.

   Hinweis: Detaillierte Anweisungen hierzu finden Sie in der Dokumentation oder Online-Hilfe von Microsoft AD.

2. Fügen Sie die Konten *emxuser2* und *usera* zur Gruppe "EMX_User" hinzu.
3. Fügen Sie die Konten *emxuser* und *userb* zur Gruppe "EMX_Admin" hinzu.
4. Überprüfen Sie, ob jede Gruppe die richtigen Benutzer umfasst.

Schritt C. Konfigurieren der LDAP-Authentifizierung auf dem EMX-Gerät

Sie müssen die LDAP-Authentifizierung auf dem EMX-Gerät richtig einrichten und aktivieren, um die externe Authentifizierung nutzen zu können.

Bei dieser Veranschaulichung gehen wir von Folgendem aus:

- Die DNS-Server-Einstellungen wurden korrekt konfiguriert. Siehe ***Ändern der Netzwerkeinstellungen*** (auf Seite 84) und ***Rolle eines DNS-Servers*** (siehe "***Funktion eines DNS-Servers***" auf Seite 88).
- Der Domänenname des AD-Servers lautet *techadssl.com* und dessen IP-Adresse *192.168.56.3*.
- Das AD-Protokoll wird NICHT über SSL verschlüsselt.
- Der AD-Server verwendet den Standard-TCP-Port *389*.
- Anonymous Bind wird verwendet.

So konfigurieren Sie die LDAP-Authentifizierung:

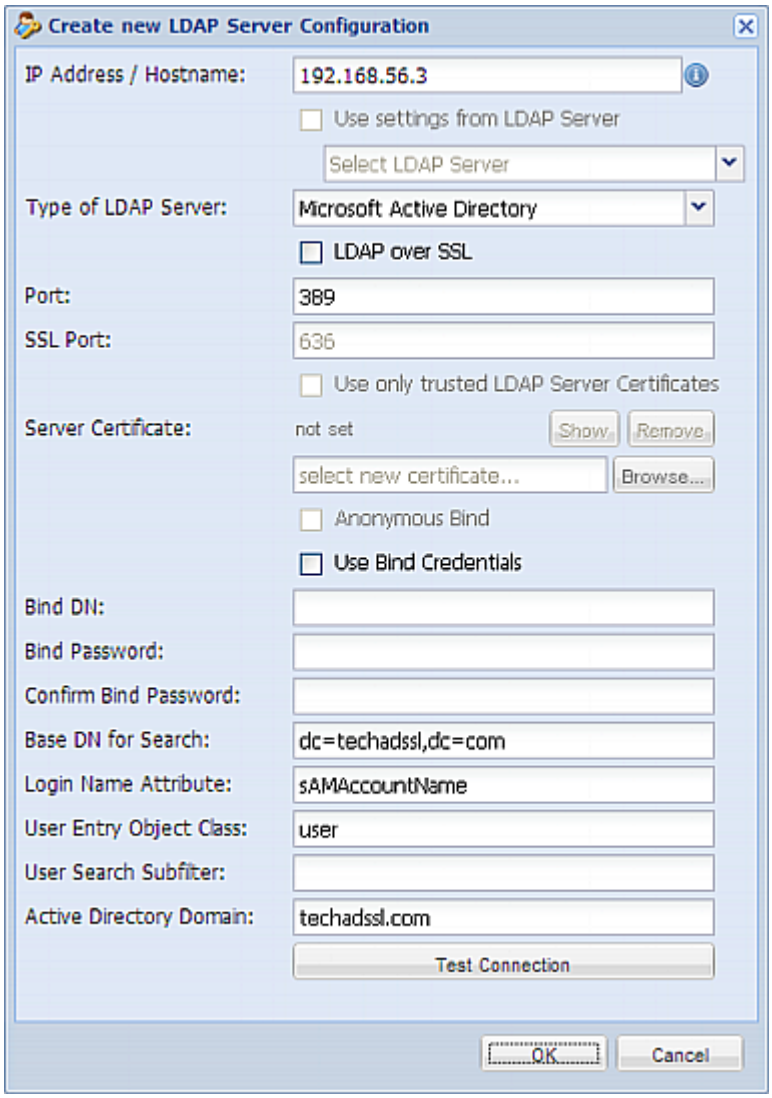
1. Wählen Sie "Device Settings" > "Security" > "Authentication" (Geräteeinstellungen > Sicherheit > Authentifizierung) aus. Das Dialogfeld "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie das Optionsfeld "LDAP" aus, um die LDAP/LDAPS-Remote-Serverauthentifizierung zu aktivieren.
3. Klicken Sie auf "New" (Neu), um einen LDAP/LDAPS-Server für die Authentifizierung hinzuzufügen. Das Dialogfeld "Create new LDAP Server Configuration" (Neue LDAP-Serverkonfiguration erstellen) wird angezeigt.
4. Stellen Sie der EMX-Einheit Informationen über den AD-Server bereit.
   - IP Address/Hostname (IP-Adresse/Hostname) – Geben Sie den Domänennamen `techadssl.com` oder die IP-Adresse `192.168.56.3` ein.

   Wichtig: Wenn die SSL-Verschlüsselung deaktiviert ist, können Sie entweder den Domänennamen oder die PI-Adresse in dieses Feld eingeben. Wenn die SSL-Verschlüsselung aktiviert ist, müssen Sie den vollständig qualifizierten Domänennamen eingeben.

   - Verwenden Sie die Einstellungen vom LDAP-Server – Lassen Sie das Kontrollkästchen deaktiviert.
   - Type of LDAP Server (Typ des LDAP-Servers) – Wählen Sie "Microsoft Active Directory" aus der Dropdown-Liste.

- LDAP over SSL (LDAP über SSL) – Lassen Sie das Kontrollkästchen deaktiviert, da bei diesem Beispiel keine SSL-Verschlüsselung erfolgt.
- Port – Stellen Sie sicher, dass das Feld auf `389` eingestellt ist.
- SSL Port and Server Certificate (SSL-Port und Serverzertifikat) – Überspringen Sie die zwei Felder, da die SSL-Verschlüsselung nicht aktiviert ist.
- Use Bind Credentials (Bind-Informationen verwenden) – Aktivieren Sie dieses Kontrollkästchen NICHT, weil ein anonymes Bind verwendet wird.
- Bind DN (Bind-DN), Bind Password (Bind-Kennwort) und Confirm Bind Password (Bind-Kennwort bestätigen) – Überspringen Sie diese drei Felder, weil ein anonymes Bind verwendet wird.
- Base DN for Search (Basis-DN für Suche) – Geben Sie `dc=techadssl,dc=com` als Ausgangspunkt ein, an dem Ihre Suche auf dem AD-Server beginnt.
- Login Name Attribute (Anmeldename-Attribut) – Stellen Sie sicher, dass das Feld auf `sAMAccountName` eingestellt ist, da der LDAP-Server vom Typ "Microsoft Active Directory" ist.
- User Entry Object Class (Objektklasse für Benutzereinträge) – Stellen Sie sicher, dass das Feld auf `user` eingestellt ist, da der LDAP-Server vom Typ "Microsoft Active Directory" ist.
- User Search Subfilter (Subfilter für Benutzersuche) – Dieses Feld ist optional. Die Subfilterinformationen sind hilfreich, um zusätzliche Objekte in einer großen Verzeichnisstruktur herauszufiltern. In diesem Beispiel bleibt es leer.

- Active Directory Domain (Active Directory-Domäne) – Geben Sie `techadssl.com` ein.



Hinweis: Für weitere Informationen zur LDAP-Konfiguration siehe **Einrichten der LDAP-Authentifizierung** *(auf Seite 129).*

5. Klicken Sie auf "OK", um die Änderungen zu speichern. Der LDAP-Server wird gespeichert.
6. Klicken Sie auf "OK", um die Änderungen zu speichern. Die LDAP-Authentifizierung wird aktiviert.

Hinweis: Wenn die Uhr von EMX und die des LDAP-Servers nicht mehr synchronisiert sind, werden die Zertifikate als abgelaufen betrachtet und die Benutzer können nicht mithilfe von LDAP authentifiziert werden. Um eine ordnungsgemäße Synchronisierung sicherzustellen, sollten Administratoren die EMX-Einheit und den LDAP-Server so konfigurieren, dass sie denselben NTP-Server verwenden.

Schritt D. Konfigurieren der Benutzergruppen auf dem EMX-Gerät

Eine Rolle auf dem EMX-Gerät bestimmt die Systemberechtigungen. Sie müssen Rollen erstellen, deren Namen den für die EMX-Einheit auf dem AD-Server erstellten Benutzergruppen entsprechen, da die Authentifizierung andernfalls fehlschlägt. Wir erstellen daher die Rollen *EMX_User* und *EMX_Admin* auf dem EMX-Gerät.

Bei dieser Veranschaulichung gehen wir von Folgendem aus:

- Der Rolle *EMX_User* zugewiesene Benutzer können nur auf das EMX-Gerät zugreifen und Einstellungen anzeigen.
- Der Rolle *EMX_Admin* zugewiesene Benutzer können auf das EMX-Gerät zugreifen und es konfigurieren, weil sie über Administratorberechtigung verfügen.

So erstellen Sie die Rolle "EMX_User" mit den entsprechenden zugewiesenen Berechtigungen:

1. Wählen Sie "User Management" > "Roles" (Benutzerverwaltung > Benutzerfunktionen) aus. Das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) wird angezeigt.

   Tipp: Sie können das Dialogfeld "Manage Roles" (Benutzerfunktionen verwalten) auch aufrufen, indem Sie im Dialogfeld "Edit User 'XXX'" (Benutzer 'XXX' bearbeiten) auf die Schaltfläche "Manage Roles" (Benutzerfunktionen verwalten) klicken.

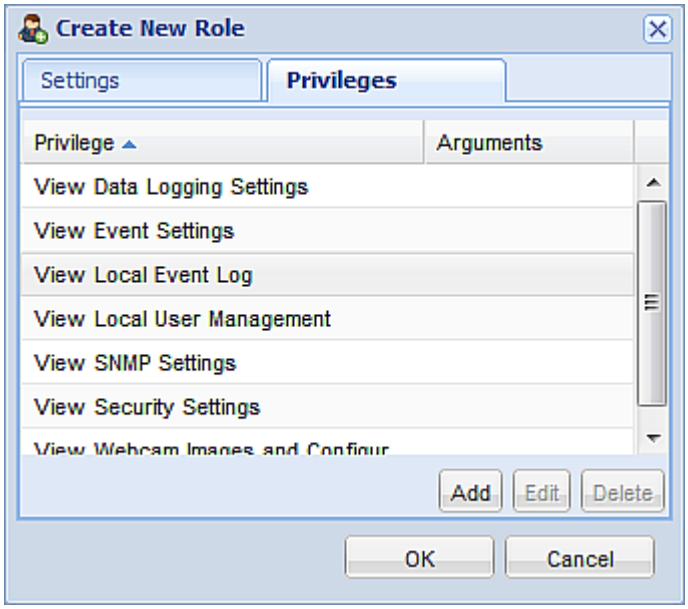
2. Klicken Sie auf "New" (Neu). Das Dialogfeld "Create New Role" (Neue Benutzerfunktion erstellen) wird angezeigt.
3. Geben Sie `EMX_User` in das Feld "Role Name" (Rollenname) ein.
4. Geben Sie im Feld "Description" (Beschreibung) eine Beschreibung für die Rolle "EMX_User" ein. In diesem Beispiel geben wir "Die Rolle kann nur EMX-Einstellungen anzeigen" als Beschreibung der Rolle ein.
5. Klicken Sie auf die Registerkarte "Privileges" (Berechtigungen), um alle Berechtigungen "View XXX" (XXX anzeigen) auszuwählen (wobei XXX für den Namen der Einstellung steht). Mit der Berechtigung "View XXX" (XXX anzeigen) können Benutzer die XXX-Einstellungen anzeigen, ohne diese konfigurieren oder ändern zu können.

a. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Privileges to new Role" (Berechtigungen zur neuen Benutzerfunktion hinzufügen) wird angezeigt.

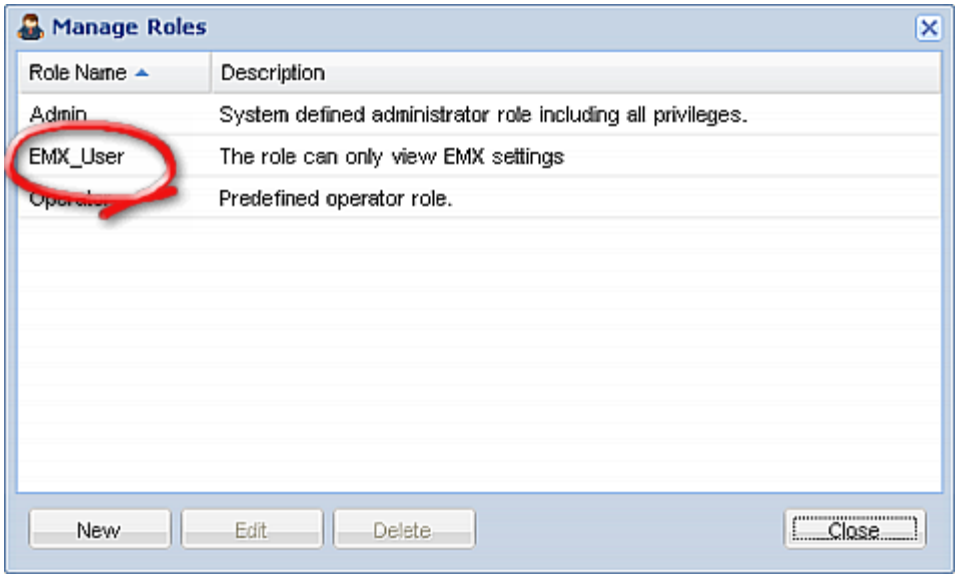
b. Wählen Sie eine Berechtigung, die mit dem Wort "View" (Anzeigen) beginnt, aus der Liste aus, z. B. "View Event Settings" (Ereigniseinstellungen anzeigen).

c. Klicken Sie auf "Add" (Hinzufügen).

d. Wiederholen Sie Schritt A bis C, um alle Berechtigungen hinzuzufügen, die mit "View" (Anzeigen) beginnen.



6. Klicken Sie auf "OK", um die Änderungen zu speichern. Die Rolle "EMX_User" wird erstellt.

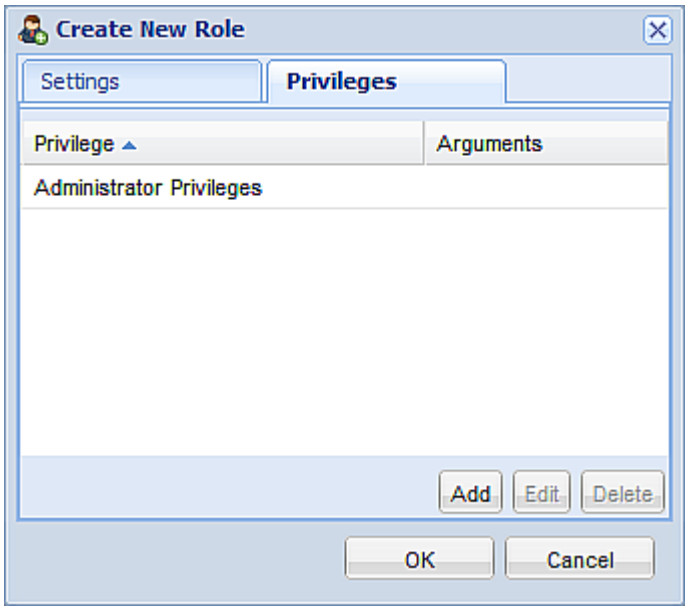


7. Lassen Sie das Dialogfeld "Manage Roles" (Rollen verwalten) geöffnet, um die Rolle "EMX_Admin" zu erstellen.

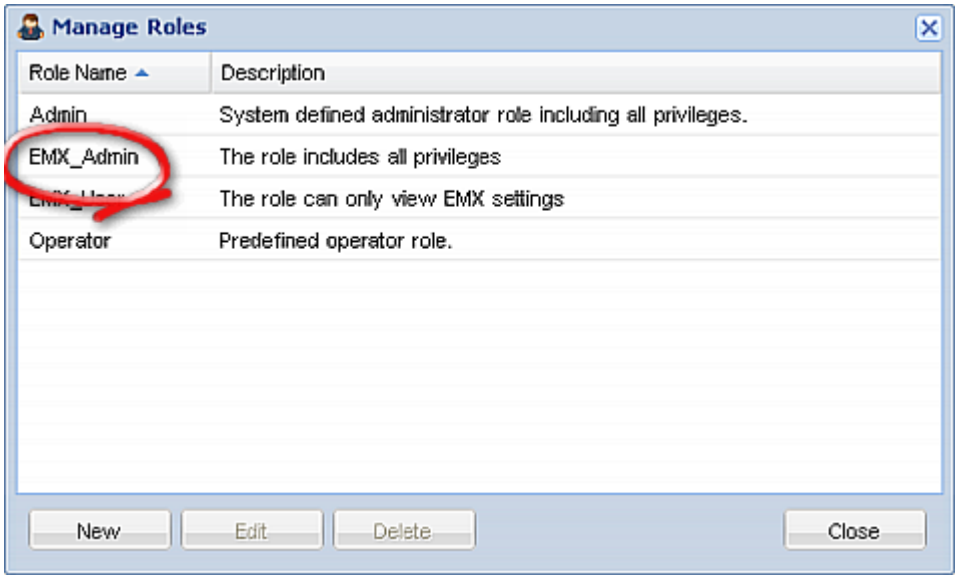
So erstellen Sie die Rolle "EMX_Admin" mit uneingeschränkten Berechtigungen:

1. Klicken Sie auf "New" (Neu). Das Dialogfeld "Create New Role" (Neue Benutzerfunktion erstellen) wird angezeigt.
2. Geben Sie `EMX_Admin` in das Feld "Role Name" (Rollenname) ein.
3. Geben Sie im Feld "Description" (Beschreibung) eine Beschreibung für die Rolle "EMX_Admin" ein. In diesem Beispiel geben wir "Die Rolle umfasst alle Berechtigungen" als Beschreibung der Rolle ein.
4. Klicken Sie auf die Registerkarte "Privileges" (Berechtigungen), um die Berechtigung "Administrator" (Administrator) auszuwählen. Die Berechtigung "Administrator" (Administrator) erlaubt den Benutzern, alle Einstellungen von EMX zu konfigurieren oder ändern.
   a. Klicken Sie auf "Add" (Hinzufügen). Das Dialogfeld "Add Privileges to new Role" (Berechtigungen zur neuen Benutzerfunktion hinzufügen) wird angezeigt.
   b. Wählen Sie die Berechtigung "Administrator Privileges" (Administratorrechte) aus der Liste "Privileges" (Berechtigungen) aus.

c. Klicken Sie auf "Add" (Hinzufügen).



5. Klicken Sie auf "OK", um die Änderungen zu speichern. Die Rolle "EMX_Admin" wird erstellt.



6. Klicken Sie auf "Close" (Schließen), um das Dialogfeld zu schließen.

Index

A

Abfragen der DNS-Server - 334
Abfragen verfügbarer Parameter für einen Befehl - 228, 337
Abmelden - 51
Abmelden bei der CLI - 338
Abrufen vorheriger Befehle - 337
Aktiveren oder Deaktivieren von SNMP v1/v2c - 266
Aktivieren der Benutzersperrung - 113
Aktivieren der Datenprotokollierung - 182
Aktivieren der Dienstbekanntmachung - 92
Aktivieren der Firewall - 105
Aktivieren der Funktion - 116, 117
Aktivieren der Kennworterneuerung - 116
Aktivieren der LDAP- und lokalen Authentifizierungsdienste - 136
Aktivieren oder Deaktivieren des Datenprotokollierung - 243
Aktivieren oder Deaktivieren eines Benutzerprofils - 306
Aktivieren oder Deaktivieren sicherer Kennwörter - 281
Aktivieren oder Deaktivieren von SNMP v3 - 266
Aktivieren oder Deaktivieren von SSH - 264
Aktivieren oder Deaktivieren von Telnet - 263
Aktivieren und Deaktivieren der Unterstützung für Schroff LHX-Wärmetauscher - 80, 210, 221
Aktivieren von Anmeldebeschränkungen - 114
Aktivieren von IPv4 oder IPv6 - 245
Aktivieren von sicheren Kennwörtern - 115
Aktivieren von SNMP - 181, 217
Aktualisieren der Assetsensor-Firmware - 99
Aktualisieren der Firmware - 97
Alarmstatus und LHX-Ereignisprotokoll - 214
Alle Berechtigungen - 317, 320, 321
Ändern der Ansicht der Benutzerliste - 68
Ändern der Benutzerfunktionen - 311
Ändern der Farbeinstellungen einer bestimmten LED - 194
Ändern der Geschwindigkeit der LAN-Schnittstelle - 261
Ändern der HTTP(S)-Einstellungen - 89
Ändern der IPv4-Einstellungen - 86
Ändern der IPv6-Einstellungen - 87
Ändern der Maßeinheiten - 77, 78, 312
Ändern der Netzwerkdiensteinstellungen - 89, 224, 226
Ändern der Netzwerkeinstellungen - 54, 84, 346
Ändern der Netzwerkkonfiguration - 14, 81
Ändern der Netzwerkschnittstelleneinstellungen - 81
Ändern der Parameter für die Firewall-Steuerung - 270
Ändern der persönlichen Daten eines Benutzers - 305
Ändern der Sensorbeschreibung - 296
Ändern der SNMPv3-Einstellungen - 307
Ändern der SSH-Einstellungen - 65, 90
Ändern der SSH-Konfiguration - 264
Ändern der Standardrichtlinie - 105, 106, 116, 117
Ändern der Telnet-Einstellungen - 91
Ändern der Telnet-Konfiguration - 263
Ändern des eigenen Kennworts - 316
Ändern des Gerätenamens - 241
Ändern des HTTP-Ports - 262
Ändern des HTTPS-Ports - 262
Ändern des Kennworts - 52
Ändern des LAN-Duplex-Modus - 261
Ändern des Sensornamens - 292
Ändern des SSH-Ports - 264
Ändern des Telnet-Ports - 263
Ändern einer Aktion - 165
Ändern einer Ereignisregel - 164
Ändern einer Firewall-Regel - 274
Ändern einer Regel für die rollenbasierte Zugriffssteuerung - 289
Ändern eines Benutzerkennworts - 304
Ändern von Benutzerfunktionen - 66, 67, 71, 319
Ändern von Benutzerprofilen - 52, 67, 71, 304
Ändern von Parametern für die rollenbasierte Zugriffssteuerung - 285
Angeben der Anzahl an Rackeinheiten - 323
Angeben der Ausrichtung des Assetsensors - 325
Angeben der Nummerierungsverschiebung für Rackeinheiten - 324
Angeben des Nummerierungsmodus für Rackeinheiten - 323
Angeben des öffentlichen SSH-Schlüssels - 265, 314

Angeben des Sensortyps - 293
Anmeldebeschränkung - 277
Anmelden - 50
Anmelden bei der CLI - 225
Anschließen der EMX-Einheit an das Netzwerk - 13, 81, 83
Anschließen der EMX-Einheit an eine Stromquelle - 10
Anschließen der EMX-Einheit an einen Computer - 11, 103, 338
Anschließen der Umgebungssensoren (optional) - 31, 173
Anschließen von AMS-M2-Z-Assetsensoren (optional) - 26, 195
Anschließen von Assetsensoren an das EMX-Gerät - 24, 26, 191, 194, 196
Anschließen von Blade-Erweiterungsstrips - 28, 199
Anschließen von Differenzluftdrucksensoren - 38
Anschluss des Kontaktschlusssensors - 49
Anschluss einer Logitech-Webcam (optional) - 39, 202, 203
Anschluss eines Schroff LHX-Wärmetauschers (optional) - 40, 209
Anschluss von Detektoren/Switches anderer Hersteller - 33
Anschluss von Detektoren/Switches anderer Hersteller an das EMX-Gerät - 36, 49, 186, 187
Anschluss von externen Detektoren/Switches an DPX-CC2-TR - 34
Anschluss-Ports - 41
Anzeigen der Geräteinformationen - 75
Anzeigen der Netzwerkverbindungen - 334
Anzeigen der Übersicht - 212
Anzeigen der verbundenen Benutzer - 68
Anzeigen des Dashboards - 61
Anzeigen des Kommunikationsprotokolls - 55, 168
Anzeigen des lokalen Ereignisprotokolls - 167
Anzeigen des Protokolls zur Firmwareaktualisierung - 98
Anzeigen von Assetsensoren - 79
Anzeigen von Details - 213
Anzeigen von Informationen - 228
Anzeigen von LHX-Wärmetauschern - 80
Anzeigen von Sensordaten - 183
Anzeigen von Webcam-Momentaufnahmen und -Videos - 204
Asset-Management bei Dominion PX - 339
Asset-Management-Informationen - 47
Assetsensoren und -Tags - 191
Aufheben der Sperrung eines Benutzers - 113, 331
Aufheben der Verwaltung von Umgebungssensoren - 177, 188
Auflisten von TCP-Verbindungen - 101
Aufrufen des Diagnosemodus - 227, 333
Aufrufen des Konfigurationsmodus - 227, 240, 251, 304, 315, 316
Auswahl des Internetprotokolls - 85, 86, 87
Auswählen der IPv4- oder IPv6-Adressen - 246
Automatisches Vervollständigen eines Befehls - 337

B

Bearbeiten der LDAP-Servereinstellungen - 134
Bearbeiten von benutzerfunktionsbasierten Zugriffssteuerungsregeln - 120
Bearbeiten von Firewall-Regeln - 110
Bearbeitung der Einstellungen zur Ping-Überwachung - 172
Bedienelemente - 45
Beenden des Diagnosemodus - 336
Beenden des Konfigurationsmodus - 241, 331
Befehl - 228
Befehle für die Konfiguration von Umgebungssensorschwellenwerten - 296
Befehle für die Netzwerkkonfiguration - 244
Befehle für die Sicherheitskonfiguration - 268
Befehle für die Umgebungssensorkonfiguration - 292
Befehle zur Assetverwaltung - 322
Befehle zur Benutzerkonfiguration - 302
Befehle zur Gerätekonfiguration - 241
Befehle zur Konfiguration von Benutzerfunktionen - 317
Befehlsverlauf - 238
Behebung von Netzwerkproblemen - 99, 333
Beispiel - 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 271, 273, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 286, 288, 291, 292, 293, 294, 295, 296, 297, 298, 300, 301, 302, 303, 304, 305, 306, 307, 311, 312, 313, 315, 316, 319, 321, 322, 323, 324, 325, 326, 327, 328, 329, 334, 335, 336

Beispiel 1 – Allgemeine Sicherheitsinformationen - 239
Beispiel 1 – Kombination aus IP-, Subnetzmaske- und Gateway-Parametern - 330
Beispiel 2 – Detaillierte Sicherheitsinformationen - 240
Beispiel 2 – Kombination von SSID- und PSK-Parametern - 331
Beispiele - 239
Beispiel-Ereignisregel auf Asset-Management-Ebene - 161
Beispiel-Ereignisregel auf Benutzeraktivitätsebene - 163
Beispiel-Ereignisregel auf Sensorebene - 162
Beispiel-Ereignisregeln - 161
Benennen des EMX-Geräts - 54, 74, 77, 176, 177, 179, 184, 188, 210, 213
Benennen einer Rackeinheit - 326
Benennen eines Assetsensors - 322
Benennen eines Wärmetauschers - 210
Benutzersperrung - 279
Bereitstellen des CA-Zertifikats für EAP - 250
Beschränkung auf Einzelanmeldung - 277
Beschreibung der Sensorposition - 178, 180
Bestehende Benutzerfunktionen - 236
Bestehende Benutzerprofile - 235
Betriebsstunden - 215

C

Certificate Signing Request (CSR) - 122

D

Datenfenster - 57
Deaktivieren der LDAP-Authentifizierung - 135
Diagnosebefehle - 333
Die EMX-MIB - 220
Drahtgebundene Netzwerkeinstellungen - 82
Drahtlose Netzwerkeinstellungen - 83
Drahtloskonfiguration - 230
Durch den Browser definiertes Kontextmenü - 60

E

Einführung - 1, 41
Einführung in die Webschnittstelle - 53
Einrichten der Datenprotokollierung - 181, 243
Einrichten der LDAP-Authentifizierung - 88, 104, 129, 348
Einrichten einer EMX-Einheit mit der Sammelkonfiguration - 74, 94
Einrichten eines SSL-Zertifikats - 104, 122
Einrichten von Benutzeranmeldesteuerungen - 112
Einrichten von Benutzerfunktionen - 52, 62, 66, 70, 182
Einrichten von benutzerfunktionsbasierten Zugriffssteuerungsregeln - 116
Einschränkungen beim Verketten von AMS-M2-Z-Sensoren - 27, 191, 196, 197
Einstellen der Deassertion-Hysterese eines Sensors - 301
Einstellen der IPv4-Adresse - 254
Einstellen der IPv4-Subnetzmaske - 254
Einstellen der IPv6-Adresse - 258
Einstellen der Netzwerkdienstparameter - 262
Einstellen der oberen Warngrenze des Sensors - 298
Einstellen der Parameter für ein drahtloses Netzwerk - 246
Einstellen der unteren Warngrenze des Sensors - 299, 300
Einstellen der X-Koordinate - 294
Einstellen der Y-Koordinate - 294
Einstellen der Z-Koordinate - 242, 295
Einstellen des Assertionszeitlimits eines Sensors - 302
Einstellen des bevorzugten Host-Namens - 253
Einstellen des IPv4-Gateways - 255
Einstellen des IPv4-Konfigurationsmodus - 253
Einstellen des IPv6-Gateways - 258
Einstellen des IPv6-Konfigurationsmodus - 257
Einstellen des oberen kritischen Schwellenwerts für den Sensor - 296
Einstellen des primären IPv4-DNS-Servers - 255
Einstellen des primären IPv6-DNS-Servers - 259
Einstellen des sekundären IPv4-DNS-Servers - 256
Einstellen des sekundären IPv6-DNS-Servers - 259
Einstellen des Z-Koordinatenformats - 179
Einstellen des Z-Koordinatenformats für Umgebungssensoren - 242, 295
Einstellen von Datum und Uhrzeit - 75
Einstellungen für einen Blade-Erweiterungsstrip - 238
Einstellungen von Assetsensoren - 231

Einstellungen von Rackeinheiten eines Assetsensors - 237
EMX2-111 - 3
EMX2-888 - 3
EMX-Geräteverwaltung - 74
Ereignisprotokollierung - 166
Ereignisregeln und Aktionen - 90, 93, 137, 151, 189, 202, 219
Ereignisregeln, Ereignisaktionen und Anwendungsprotokolle - 137
Erfassen, Anzeigen und Verwalten von Webcam-Momentaufnahmen - 202, 205
Erforderliche Angabe einer Ziffer - 283
Erforderliche Angabe eines Großbuchstabens - 283
Erforderliche Angabe eines Kleinbuchstabens - 282
Erforderliche Angabe eines Sonderzeichens - 284
Ermitteln der LDAP-Informationen - 129
Erstellen einer Benutzerfunktion - 66, 70, 317
Erstellen einer Ereignisregel - 138
Erstellen eines Certificate Signing Request (CSR) - 123
Erstellen eines selbstsignierten Zertifikats - 125
Erstellen von Aktionen - 143, 149, 208
Erstellen von benutzerdefinierten E-Mail-Nachrichten - 146, 149
Erstellen von benutzerfunktionsbasierten Zugriffssteuerungsregeln - 116, 118
Erstellen von Benutzerprofilen - 50, 62, 67, 70, 71, 78, 91, 219, 303
Erstellen von Firewall-Regeln - 105, 107
Erstellen von Regeln - 138
Erstkonfiguration des Netzwerks - 14
Erweitern eines Blade-Erweiterungsstrips - 197
Erzwingen der HTTPS-Verschlüsselung - 89, 104, 122
Erzwingen einer Kennwortänderung - 306

F

Faktoren zur Höhenkorrektur (EMX) - 77, 341
Festlegen der Anzeige von Elementen in der Verzeichnisstruktur - 79, 80
Festlegen der äußeren Authentifizierung - 248
Festlegen der Authentifizierungsmethode - 247
Festlegen der BSSID - 252
Festlegen der EAP-Identität - 249
Festlegen der EAP-Parameter - 248
Festlegen der Größe eines Verlaufspuffers - 330
Festlegen der Höhe des Geräts über Normal-Null - 77
Festlegen der inneren Authentifizierung - 249
Festlegen der LAN-Schnittstellenparameter - 260
Festlegen der LED-Farbe für - 328
Festlegen der Lese-Community für SNMP - 267
Festlegen der Messungen für die Datenprotokollierung pro Eintrag - 243
Festlegen der Schreib-Community für SNMP - 267
Festlegen der SNMP-Konfiguration - 265
Festlegen der SSH-Authentifizierungsmethode - 265, 315
Festlegen der SSID - 247
Festlegen des EAP-Kennworts - 250
Festlegen des LED-Betriebsmodus - 327
Festlegen des Netzwerkmodus - 244
Festlegen des sysContact-Werts - 267
Festlegen des sysLocation-Werts - 268
Festlegen des sysName-Werts - 268
Festlegen einer LED-Farbe für eine Rackeinheit - 327, 328
Festlegen eines LED-Modus für eine Rackeinheit - 327, 329
Festlegen von PSK - 248
Festlegen von Umgebungssensoren - 174, 176
Firewall-Steuerung - 269
Firmware-Upgrade - 96
Funktion eines DNS-Servers - 88, 346

G

Gelb oder Rot hervorgehobene Ergebnisse - 58, 61, 183, 213
Gerätestatus und Symbolwechsel - 81, 214, 216
Größe des Verlaufspuffers - 239
GSM-Modems - 208

H

Herunterladen einer SNMP-MIB - 218, 220
Herunterladen von Diagnoseinformationen - 101
Herunterladen von Schlüssel- und Zertifikatsdateien - 128

Hinweis zu nicht ausgelösten Regeln - 166
Hinzufügen der LDAP-Servereinstellungen - 130
Hinzufügen einer Firewall-Regel - 271
Hinzufügen einer Regel für die rollenbasierte Zugriffssteuerung - 287
Hinzufügen von IT-Geräten zur Ping-Überwachung - 170
HTTPS-Zugriff - 276

I

Informationen zu Kontaktschlusssensoren - 33
Informationen zum Aktualisierungsintervall - 31, 176, 181, 183
Informationen zum Umgebungssensor - 46, 232, 233
Informationen zur Schnittstelle - 224
Installieren des USB-Seriell-Treibers - 12
Installieren eines von der Zertifizierungsinstanz signierten Zertifikats - 125
Installieren und Konfigurieren des EMX-Geräts - 6
Installieren vorhandener Schlüssel- und Zertifikatsdateien - 127
Intervall der Kennworterneuerung - 278
IP Address (IP-Adresse) - 49
IP-Konfiguration - 229

K

Kennworterneuerung - 278
Komponenten einer Ereignisregel - 138
Konfiguration der Rackeinheiten - 325
Konfigurieren der Benutzer für die verschlüsselte SNMP-V3-Kommunikation - 218
Konfigurieren der EMX-Einheit - 11, 84
Konfigurieren der Firewall - 105
Konfigurieren der IP-Protokolleinstellungen - 245
Konfigurieren der IPv4-Parameter - 253
Konfigurieren der IPv6-Parameter - 257
Konfigurieren der SMTP-Einstellungen - 93, 145, 146
Konfigurieren der SNMP-Einstellungen - 64, 90
Konfigurieren des Assetsensors - 26, 191
Konfigurieren eines Kontaktschlusssensors - 35, 186, 187
Konfigurieren von EMX-Gerät und Netzwerk - 240
Konfigurieren von SNMP-Traps - 219
Konfigurieren von Temperatur- und Lüfterschwellenwerten - 189, 211
Konfigurieren von Umgebungssensoren - 33, 59, 174, 177, 189
Konfigurieren von Webcams - 39, 203, 204, 205, 207
Kopieren einer EMX-Konfiguration - 96

L

LAN-Schnittstelleneinstellungen - 229
Layout - 222
LCD-Anzeige - 43, 46, 47
LCD-Anzeigefeld - 43
LEDs des Kontaktschlusssensors - 37, 49
Löschen der Einstellungen zur Ping-Überwachung - 172
Löschen der LDAP-Servereinstellungen - 135
Löschen einer Benutzerfunktion - 73, 321
Löschen einer Ereignisregel oder Aktion - 166
Löschen einer Firewall-Regel - 275
Löschen einer Regel für die rollenbasierte Zugriffssteuerung - 291
Löschen von benutzerfunktionsbasierten Zugriffssteuerungsregeln - 121
Löschen von Benutzerprofilen - 68, 315
Löschen von Ereigniseinträgen - 168
Löschen von Firewall-Regeln - 112

M

MAC-Adresse - 48
Maximale Kennwortlänge - 282
Maximale Umgebungstemperatur für den Betrieb (EMX) - 342
Maximaler Kennwortverlauf - 284
Menüs - 54
Mindestlänge eines Kennworts - 281
Mit HyperTerminal - 225, 331
Mit SSH oder Telnet - 226
Montage eines 1U-EMX-Geräts - 8
Montage eines Null-U-EMX-Geräts - 7
Montieren des EMX-Geräts - 6
Multi-Befehlssyntax - 271, 277, 280, 281, 286, 304, 305, 307, 312, 330

N

Netzschalter - 49
Netzwerkdiagnose - 99
Netzwerkdiensteinstellungen - 230
Netzwerkkonfiguration - 228
Netzwerkmodus - 229

Neustart des EMX-Geräts - 102
Neustart des Geräts - 332

P

Paketinhalt - 5
Pinbelegung des RS-485-Ports - 343
Pinbelegung des seriellen RS-232-Ports - 342
Platzhalter in E-Mail-Nachrichten - 149, 150
Produktfeatures - 4
Produktmodelle - 3

R

Reset-Taste - 49
RJ-12-Pin-Belegung - 342
Rollenbasierte Zugriffssteuerung - 285

S

Schaltfläche - 54
Schließen einer seriellen Verbindung - 227
Schritt A. Festlegen der Benutzerkonten und Gruppen - 344
Schritt B. Konfigurieren der Benutzergruppen auf dem AD-Server - 345
Schritt C. Konfigurieren der LDAP-Authentifizierung auf dem EMX-Gerät - 346
Schritt D. Konfigurieren der Benutzergruppen auf dem EMX-Gerät - 349
Schroff LHX-Wärmetauscher - 40, 58, 209
Schwellenwertinformationen - 189, 223
Schwellenwertinformationen zum Umgebungssensor - 234
Security (Sicherheit) - 104
Security Settings (Sicherheitseinstellungen) - 235
Senden von Videos in einer E-Mail oder Sofortnachricht - 202, 207
Sensormessgenauigkeit - 184
Serverzugriff - 170
Sichere Kennwörter - 281
SNMP-GET- und SET-Befehle - 220
SNMP-SET-Befehle und Schwellenwerte - 223
Sortieren der Reihenfolge für den LDAP-Zugriff - 133
Sortieren von benutzerfunktionsbasierten Zugriffssteuerungsregeln - 121
Sortieren von Firewall-Regeln - 111
Speichern einer EMX-Konfiguration - 95
Spezifikationen - 341
Standard-Protokollnachrichten - 146, 151
Status - 186, 187, 188
Status verwalteter Sensoren - 185
Statusleiste - 54
Steuern des Wärmetauschers - 215
Symbol - 56

T

Testen der LDAP-Serververbindung - 134
Testen der Netzwerkkonnektivität - 335

U

Überprüfen des Serverüberwachungsstatus - 173
Überprüfen eines Hosts mit dem Ping-Tool - 100
Überschreiben des über IPv4-DHCP zugewiesenen DNS-Servers - 256
Überschreiben des über IPv6-DHCP zugewiesenen DNS-Servers - 259, 260
Übersicht - 2, 62, 74, 170, 339
Überwachen des Wärmetauschers - 212, 214
Umgebungssensoren - 173
Unterschiedliche CLI-Modi und -Eingabeaufforderungen - 226, 227, 240
Unterstützte Webbrowser - 41
Unterstützte Wireless-LAN-Konfiguration - 14

V

Veranschaulichung der LDAP-Konfiguration - 133, 344
Verfolgen der Netzwerkroute - 100
Verfolgen der Route - 336
Verknüpfen von Assetsensoren - 22
Verwalten externer Geräte - 170
Verwalten von Benutzerfunktionen - 70
Verwalten von Benutzern - 62
Verwalten von Firewall-Regeln - 271
Verwalten von Regeln für die rollenbasierte Zugriffssteuerung - 287
Verwalten von Umgebungssensoren - 174, 176
Verwaltung des Assetsensors - 322
Verwaltung von Benutzern und Benutzerfunktionen - 62
Verwenden der Befehlszeilenschnittstelle - 224
Verwenden von SNMP - 98, 217
Vollständige Notfallwiederherstellung - 99
Vorbereitende Schritte - 6

W

Warnsymbol - 57
Was ist das Assertionszeitlimit? - 179, 190, 302
Was ist Deassertionshysterese? - 166, 179, 189, 212, 301
Webcams - 39, 202
Weitere Informationen zur AD-Konfiguration - 133
Wiederherstellen der werksseitigen Standardeinstellungen - 49, 103, 333
Wiederherstellen der werksseitigen Standardeinstellungen (CLI) - 338

Z

Zeitlimit für Inaktivität - 279
Zugriffssteuerung - 104
Zurücksetzen der EMX-Einheit - 332

USA/Kanada/Lateinamerika

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

China

Peking
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

Shanghai
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

GuangZhou
Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

Indien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881

Japan

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5991
E-Mail: support.japan@raritan.com

Europa

Europa
Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

Großbritannien
Montag bis Freitag
08:30 bis 17:00 Uhr GMT
Telefon +44(0)20-7090-1390

Frankreich
Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

Deutschland
Montag bis Freitag
08:30 bis 17:30 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0
E-Mail: rg-support@raritan.com

Melbourne, Australien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

Taiwan

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: support.apac@raritan.com